UNIVERSIDAD PABLO DE OLAVIDE

TESIS DOCTORAL

DOCTORADO CIENCIAS JURÍDICAS Y POLÍTICAS

"RECONOCIMIENTO TRANSFRONTERIZO DE LA FIRMA ELECTRÓNICA"

AUTOR: ANTONIO MERCHÁN MURILLO

TUTOR DIRECTOR: PROF. DR. AGUSTÍN MADRID PARRA

Sevilla, 2015.

UNIVERSIDAD PABLO DE OLAVIDE

FACULTAD DE DERECHO, DPTO. DERECHO PRIVADO,

ÁREA DE DERECHO MERCANTIL

TESIS DOCTORAL

DOCTORADO CIENCIAS JURÍDICAS Y POLÍTICAS

"RECONOCIMIENTO TRANSFRONTERIZO DE LA FIRMA ELECTRÓNICA"

Doctorando

Fdo.: Antonio Merchán Murillo

Visto Bueno tutor/director

Fdo.: Prof. Dr. Agustín Madrid Parra

Sevilla, 2015

UNIVERSIDAD PABLO DE OLAVIDE

FACULTAD DE DERECHO, DPTO. DERECHO PRIVADO,

ÁREA DE DERECHO MERCANTIL

TESIS DOCTORAL

DOCTORADO CIENCIAS JURÍDICAS Y POLÍTICAS

"RECONOCIMIENTO TRANSFRONTERIZO DE LA FIRMA ELECTRÓNICA"

AUTOR: ANTONIO MERCHÁN MURILLO

TUTOR DIRECTOR: PROF. DR. AGUSTÍN MADRID PARRA

Sevilla, 2015.

ÍNDICE

ABREVIATURAS

ABA	*American Bar Association*.
AELC	Asociación Europea de Libre Comercio.
AGC	*Attorney-General's Chambers*.
APEC	Asociación Económica de Asia y el Pacífico (*Asia Pacific Economic Cooperation*).
Art.	Artículo.
BGB	*Bürgerlichen Gesetzbuches*.
CC	Código Civil.
CCo	Código de Comercio.
CCI	Cámara de Comercio Internacional.
CNUDMI/UNCITRAL	Comisión de Naciones Unidas para el Derecho Mercantil Internacional.
CO	Certificados de Origen.
DGRN	Dirección General de Registros y del Notariado.
DNI	Documento Nacional de Identidad.
DOUE	Diario Oficial de la Unión Europea.
E-APP	*e-Apostille Pilot Program*.
e-ID	e-Identificación.
ECEG	*Electronic Commerce Expert Group*.
EDI	Intercambio Electrónico de Datos (*Electronic Data Interchange*).
EPIC	*Electronic Privacy Information Center*.
E-Sign	*Electronic Signature in Global and Nacional Commerce Act*.

ETA	*Electronic Transactions Act*.
FNMT	Fábrica Nacional de Moneda y Timbre.
GUIDEC	Guía de Uso General en el Comercio Digital Internacional (*General Usage for International Digitally Ensured Commerce*).
ICP	Infraestructura de Clave Pública.
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos.
IP	*Internet Protocol*.
IDA	*Info-Communications Development Authority of Singapore*.
IEC	Comisión Electrotécnica Internacional.
ISO	Organización Internacional de Normalización.
LEC	Ley 1/2000, de 7 de enero, de enjuiciamiento Civil.
LFE	Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
LMCE	Ley Modelo sobre Comercio Electrónico.
LMFE	Ley Modelo sobre Firma Electrónica.
LSSICE	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
NIF	Número de Identificación Fiscal.
NOIE	*National Office of the Information Economy*.
OCDE	Organización de Cooperación y Desarrollo Económico.
OACI	Organización de la Aviación Civil Internacional.
OEA	Organización de Estados Americanos.
OIT	Organización Internacional del Trabajo.
PSC	Prestador de Servicios de Certificación.
PKI	*Public Key Infrastructure*.
RAE	Real Academia de la Lengua Española.

RD	Real Decreto.
SET	*Secure Electronic Transaction*.
SSL	*Secure Soket Layer*.
SigG	*Gesetz über Rahmenbedingungen für elektronische Signaturen – Signaturgesetz*.
SWIFT	*Society for Worldwide Interbank Financial Transactions*.
TEL	Grupo de Trabajo de Telecomunicaciones de la APEC.
TFUE	Tratado de Funcionamiento de la Unión Europea.
TJUE	Tribunal de Justicia de la Unión Europea.
TIC´s	Tecnologías de la Información y la Comunicación.
UCC	*Uniform Commercial Code*.
UCITA	*Uniform Computer Information Transactions Act*.
UIT	Unión Internacional de Telecomunicaciones.
UE	Unión Europea.
UETA	*Uniform Electronic Transaction Act*.
ZPO	*Zivilprozessordnung*.

RESUMEN

Este trabajo se focaliza en el reconocimiento transfronterizo de la firma electrónica. La regulación de la firma electrónica puede contribuir al desarrollo del comercio electrónico; sin embargo, parece que la adopción de leyes y la forma en que se aplican no se están desarrollando de una manera óptima que permita el uso armonizado, a nivel internacional, de la firma electrónica y, con ella, las tecnologías que, a veces, la acompañan. En el mismo, se pretende ofrecer una amplia y profunda visión de la regulación de la firma electrónica en el mundo, con el fin de determinar si, la situación legislativa actual, facilita el desarrollo internacional del comercio electrónico o no. Con la intención de ofrecer respuestas, el autor trata de describir, de manera global, la regulación de la firma electrónica e identificar las cuestiones claves que participan en ella. El objetivo principal es proponer y ofrecer respuestas a las cuestiones que han surgido, a lo largo de los años, en la construcción de un marco global y armonizado para la firma electrónica.

ABSTRACT

This work is focused on the cross-border recognition of the electronic signature. The regulation of electronic signatures could contribute to the development of electronic commerce. However it seems that the adoption of numerous laws and the way they are being implemented, are not developing in a way that would optimise the use of electronic signatures, internationally, and with it the technologies that, sometimes, accompany. In this work, we intend to find a broad and deep view of electronic signatures regulation in the world, in order to determine whether the current legislative status facilitates the electronic commerce development or not. Our intention is to offer answers, the author tries to describe, globally, the regulation of electronic signatures and identify the key issues involved in it. The aim is to propose and provide answers to questions that have arisen over the years, in building a comprehensive and harmonized framework for electronic signatures.

PALABRAS CLAVE: firma electrónica; reconocimiento transfronterizo; identificación; autenticación; autorización; transacción.

KEYWORDS: electronic signature; cross-border recognition; identification; authentication; authorization; transaction.

INTRODUCCIÓN

Un gran número de transacciones comerciales se celebran internacionalmente por medio del comercio electrónico, en el que se usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel.

El hecho de que la transmisión electrónica de datos no se circunscriba solo al ámbito nacional, nos permite hablar de la necesidad de que el reconocimiento jurídico de las nuevas tecnologías deba darse en un ámbito internacional, prestando especial atención a los problemas que puedan surgir.

El comercio electrónico puede generar incertidumbres derivadas, entre otras cuestiones, de la naturaleza de los medios a través de los que se desenvuelve, planteando problemas de autenticación, integridad, rechazo y confidencialidad en las comunicaciones.

Siendo conscientes de la importancia de la firma electrónica en el cumplimiento de sus funciones de identificación, autenticación de la identidad y autorización/autenticación de la transacción en el comercio electrónico, se han intentado reducir las incertidumbres jurídicas a través de instrumentos armonizadores**.**

Teniendo en cuenta este carácter transfronterizo de las transacciones, la CNUDMI/UNCITRAL desarrolló la Ley Modelo sobre Comercio Electrónico (1996) y la Ley Modelo sobre Firma Electrónica (2001), con las que ha tratado de orientar a los Estados, para que adopten dichos modelos, a la hora de dictar normas internas en la materia, estableciendo así un marco legislativo moderno, armonizado y equitativo para abordar, de manera eficaz, dichas materias; mostrando consciencia de la gran utilidad de las nuevas tecnologías de identificación personal utilizadas en el comercio electrónico, generalmente conocidas como firmas electrónicas.

En 2005 la CNUDMI/UNICTRAL desarrolló la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales con el fin de aportar certidumbre en relación con ese valor jurídico

internacional de las comunicaciones electrónicas. Y lo hace adoptando los principios y reglas generales contenidos en las Leyes Modelos, de manera que tengan la naturaleza de derecho objetivo directamente aplicable; todo en pro de la uniformidad y armonización del Derecho aplicable a la contratación electrónica y a la firma electrónica y, con ello, a lo que se refiere en cuanto a su fiabilidad y/o seguridad, teniendo como objetivo la actividad empresarial.

Sin embargo, los Estados han promulgado Leyes, que si bien han tenido en cuenta los principios consagrados en las Leyes Modelos, se centran en necesidades y medios nacionales, generando un sistema complejo con soluciones distintas que provocan la creación de obstáculos transfronterizos, que lastran el funcionamiento del mercado para las empresas y ciudadanos a nivel internacional.

La uniformidad resulta difícil y compleja: algunos Estados adaptaron las Leyes Modelo a sus legislaciones internas[1]; otros, si bien las han tenido en cuenta, han introducido diversos criterios, que ha provocado el surgimiento de problemas al reconocimiento transfronterizo de la firma electrónica[2].

Esta situación nos ha llevado estudiar el reconocimiento transfronterizo de la firma electrónica, teniendo como punto de partida las Leyes Modelo, donde nació la idea de armonización, en lo relativo al reconocimiento de firma, como algo que dotaría de una mayor certidumbre jurídica al comercio internacional. Siguiendo el estudio con las distintas opciones, que han dado al reconocimiento transfronterizo de la firma electrónica, nos centraremos, especialmente, en la Unión Europea, en la Directiva 1999/93/CE y el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la mencionada Directiva. Asimismo, estudiaremos las cuestiones que se vienen dando, desde una perspectiva estatal, en las que analizando diferentes legislaciones y los organismos que han influido en ellas, observando los resultados obtenidos.

[1] Cabe destacar cómo la Ley Modelo también ha servido de base para la armonización interna de la legislación sobre comercio electrónico en países con una organización federal, como Estados Unidos y Australia.
[2] Por ejemplo, la Unión Europea.

Para ello, el punto de partida de nuestro estudio, con carácter introductorio, en los capítulos primero y segundo, lo hemos puesto en la existencia de un régimen normativo relativo a la firma electrónica y su evolución conceptual; surgiendo con fuerza la necesidad de proteger los datos y, con ellos, a los consumidores. El objetivo es examinar el marco normativo que se ha ido estableciendo a través las distintas iniciativas legislativas, en el plano supraestatal y en el plano estatal, haciendo hincapié, como podrá observarse, en este último, en países con diferente tradición jurídica.

Tras la constatación del marco normativo propuesto y, posteriormente, el establecido en los diferentes Estados analizaremos, en los capítulos tercero y cuarto, respectivamente, las funciones de la firma electrónica (identificación, autenticación de la identidad y autenticación/autorización de la transacción).

Ante la trascendencia que posee el valor de asignar a través de la firma electrónica la identificación, como mecanismo de verificación de la identidad de las partes y de la autorización/autenticación de la celebración de un acto jurídico verificado, que se realizará mediante medios informáticos fiables y/o seguros, neutrales y/o no neutrales, entendiendo esto último como la posibilidad de que existan ambas opciones.

En este contexto, se observarán los diferentes enfoques adoptados por los Estados: minimalista, prescriptivo y de doble nivel.

Sobre la base de la existencia de diferentes tradiciones jurídicas estatales y el impacto que tiene sobre la legislación el enfoque normativo que se desarrolla, pasamos a analizar, en los capítulos quinto y sexto, si son los derechos los que generan o propician los problemas legales en las transacciones realizadas, a través de los medios electrónicos, o lo son las leyes y sus respectivas jurisdicciones.

Por ello, trataremos de desarrollar la verdadera problemática surgida en el uso de la firma electrónica: en el establecimiento de requisitos añadidos diferentes, para determinadas firmas electrónicas (las firmas electrónicas simples), que llevan, según el caso y el Estado en que nos situemos, a obligar al Tribunal a establecer las pautas para determinar su valor probatorio, ante el no establecimiento de las mismas en la Ley; en la

prescripción de uso una determinada firma, con una determinada tecnología, en el establecimiento de un valor probatorio presuntivo, con requisitos claramente establecidos; los espacios de aplicación de los tipos de firma y el reconocimiento fuera de aquél.

En esta dinámica surge la necesidad de regular los agentes que interactúan en el mercado, centrada exclusivamente o no, según el Estado en que nos situemos, en el prestador de servicios de certificación; con ello, aparece un sistema de aseguramiento de la responsabilidad en el ejercicio de sus funciones, de carácter subjetivo y, a veces, objetivo, en tanto que la utilización de la firma electrónica puede, eventualmente, originar daños no sólo a los usuarios de sus certificados, sino también a otros sujetos que actúen de buena fe.

A través del Derecho Internacional Privado trataremos de globalizar las distintas respuestas, que nacen en la gestión de la responsabilidad, situadas en la esfera privada de cada persona, física o jurídica, que va a interactuar en el mercado. La perspectiva jurídica que se viene a plantear será fruto de una problemática concreta, que deberá aplicarse siempre a los casos en los que, quién realiza una transacción, en un determinado país, tiene su propia legislación y, a la vez, un espacio donde se aplica; pero al interactuar con otra persona o entidad, ésta, también, tiene su propia legislación. Esto nos situará en la disyuntiva de no saber qué disposiciones utilizar, situándonos en la problemática de las normas conflicto.

CAPÍTULO PRIMERO: PRESUPUESTOS NORMATIVOS

1.1. Plano supraestatal

1.1.1. Ámbito universal

1.1.1.1. CNUDMI/UNCITRAL

1.1.1.1.1. Leyes Modelo

El 12 de junio de 1996, la CNUDMI aprobó la Ley Modelo sobre Comercio Electrónico[3] con objeto de posibilitar y facilitar el comercio por medios electrónicos ofreciendo a los legisladores un conjunto de reglas internacionalmente aceptables encaminadas a suprimir los obstáculos jurídicos y a dar una mayor previsibilidad al comercio electrónico. En particular, la Ley Modelo tiene la finalidad de superar los obstáculos que plantean las disposiciones legislativas y que no pueden modificarse mediante contrato, equiparando el trato dado a la información sobre papel al trato dado a la información electrónica. Esa igualdad de tratamiento es esencial para hacer posibles las comunicaciones sin soporte de papel y para fomentar así la eficacia en el comercio internacional[4].

De esta forma, se trata de ayudar a remediar los inconvenientes que dimanan del hecho, de que un régimen legal interno inadecuado, puede obstaculizar el comercio internacional, al depender una parte importante de ese comercio de la utilización de las modernas técnicas de comunicación. La diversidad de los regímenes internos aplicables a esas técnicas de comunicación y la incertidumbre a que dará lugar esa disparidad puede contribuir a limitar el acceso de las empresas a los mercados internacionales.

[3] Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). Fecha de adopción: 12 de junio de 1996 (el artículo 5 bis suplementario fue adoptado en 1998).
Disponible en: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html (última visita: 31/5/2014).

[4] CNUDMI/UNCITRAL: *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, 1999, párr. 1.

Por ello, la Ley Modelo sobre Comercio Electrónico se enuncian los procedimientos y principios básicos, a la vez que fundamentales, para facilitar el empleo de las técnicas modernas de comunicación, con objeto de consignar y comunicar la información en diversos tipos de circunstancias, tales como: la no discriminación, la neutralidad respecto de los medios técnicos y la equivalencia funcional, principios ampliamente reconocidos como elementos fundamentales del comercio electrónico[5]. Estos principios se ven reflejados en la enunciación de los requisitos que deben cumplir las comunicaciones electrónicas, para alcanzar los mismos fines y desempeñar las mismas funciones que se persiguen en el sistema tradicional basados en el papel con determinados conceptos, como los de "escrito", "original", "firma", y "documento"[6].

En concreto, respecto de la firma, en la creciente utilización de técnicas electrónicas de autenticación, en sustitución de las firmas manuscritas de otros procedimientos tradicionales de autenticación, se creó la necesidad de establecer un marco jurídico específico que redujese la incertidumbre de los efectos jurídicos que pueden tener la utilización de medios electrónicos[7]. Se planteó, así, la necesidad de crear un nuevo marco jurídico específico, para reducir la incertidumbre con respecto a las consecuencias legales que pudieran derivarse del empleo de la nueva situación técnica.

En este marco, se diferenciaron dos tipos de incompatibilidades: técnicas, que afectan a la interoperabilidad de los sistemas de autentificación; y jurídicas, que pueden surgir cuando las leyes de los ordenamientos nacionales estipulen diferentes requisitos en cuanto a la utilización y validez de los métodos de firma y autentificación electrónica[8]. Las incompatibilidades jurídicas y técnicas son las dos principales causas

[5] ILLESCAS ORTÍZ, R.: *Derecho de la Contratación Electrónica*, Madrid, 2011, págs. 31 y ss.
[6] Artículos 5 a 10 del Capítulo II "Aplicación de los requisitos jurídicos a los mensajes de datos" de la Ley Modelo sobre Comercio Electrónico (1996).
[7] MADRID PARRA, A.: "Regulación internacional del comercio electrónico: examen comparado de las leyes modelo de UNCITRAL", *Revista Aranzadi de Derecho de las Nuevas Tecnologías*, núm. 2, 2003, págs.15-41.
[8] Decisión 2004/387CE de la Comisión de 28 de Abril de 2004: define la interoperabilidad como "la capacidad de los sistemas y de las comunicaciones (TIC) y de los procesos empresariales a los que se apoyen, de intercambiar datos y posibilitar la puesta en común de información y conocimientos". De esta forma, hace ver como la interoperabilidad atiende a los siguientes aspectos: a) Política, relacionada con la voluntad de los países; b) Organizativos, relacionado con las redes que se desean conseguir; c) Semántica, que la información que se intercambie sea entendida por otra aplicación que no fue diseñada

de dificultad en la utilización transfronteriza de los métodos de firma y autentificación electrónica[9].

Cuando la legislación interna admite formas electrónicas equivalentes a los métodos de autentificación basados en soporte papel, es posible que sean incompatibles los criterios de validez de esas formas electrónicas equivalentes. Por ejemplo, si la ley reconoce solo las firmas digitales, no serán aceptables otras formas de firma electrónica. Puede ser que, otras discrepancias en los criterios de reconocimiento de los métodos de autentificación y firma electrónica, no impidan en principio su utilización a través de las fronteras, pero sí que reduzcan sus ventajas de rapidez y eficiencia[10].

En este contexto se presenta en 2001 la Ley Modelo de la CNUDMI sobre Firma Electrónica[11], texto que se recomienda a los Estados para su incorporación al derecho interno, con unos principios básicos, que han de ser respetados para obtener una armonización a nivel internacional. Estos principios son: neutralidad tecnológica, no discriminación entre las firmas electrónicas nacionales y extranjeras, la autonomía de las partes y el origen internacional de la Ley[12]. Esta Ley Modelo tiene por finalidad ofrecer unos principios fundamentales que faciliten el empleo de las firmas electrónicas, pero sin establecer en si misma todas las normas y reglamentaciones que pueden ser necesarias para aplicar dichas técnicas en un Estado promulgante[13].

---

inicialmente para este propósito; d) Técnica, preocupación por los problemas que existen para intercomunicar sistemas y servicios heterogéneos. Esta tiene aspectos claves como el uso de interfaces y estándares abiertos, servicios de interconexión, integración de datos, middleware, presentación de datos e intercambio de información, accesibilidad y la garantía de seguridad de los servicios; e) Jurídica, relacionada con los leyes reguladoras de la firma electrónica.

[9] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 145.

[10] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 146.

[11] Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). Fecha de adopción: 5 de julio de 2001. Disponible en:
http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2001Model_signatures.html (última visita: 31/5/2014).

[12] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE*, Nueva York, 2002, párr. 67 y ss.

[13] MADRID PARRA, A.: "Ley modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista Aranzadi de Derecho Patrimonial*, núm. 11, 2003, págs. 31-64.

1.1.1.1.2. Convención de Naciones Unidas sobre la Utilización de las Conminaciones Electrónicas en los Contratos Internacionales

Ante los obstáculos y problemas formales creados por la incertidumbre, en cuanto a los valores jurídicos de las comunicaciones electrónicas intercambiadas en el ámbito de los contratos internacionales, que constituyen una dificultad para el comercio internacional, se consideró conveniente la adopción de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[14] que establece normas uniformes para eliminar los obstáculos que se oponen al uso de las comunicaciones electrónicas en los contratos internacionales.

De esta manera, se trata de aumentar la certidumbre jurídica que se ha ido estableciendo entre la forma electrónica y la forma escrita, para facilitar la utilización de las comunicaciones electrónicas en el comercio internacional. La CNUDMI quiere fomentar la armonización de las reglas aplicables al comercio electrónico y promover la uniformidad en la adopción de instrumentos nacionales basados en Leyes Modelo de la CNUDMI sobre Comercio Electrónico y Firma Electrónica, así como actualizar y complementar ciertas disposiciones de estas Leyes teniendo en cuenta las prácticas jurídicas recientes[15].

La Convención, con miras a aumentar la certidumbre jurídica y la previsibilidad comercial, en el deseo de encontrar una solución común para eliminar los obstáculos jurídicos[16] que se oponen al uso de las comunicaciones electrónicas para los Estados con sistemas jurídicos, sociales y económicos diferentes[17], les ofrece disposiciones

[14] Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005). Fecha de adopción: 23 de noviembre de 2005. Disponible en: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention.html (última visita: 31/5/2014).

[15] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 45 y ss.

[16] OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, pág. 45-88.

[17] Como comenta el Prof. Madrid Parra: "El avance del Grupo de Trabajo en torno a disposiciones consensuadas fue realmente lento. Las posiciones de las Delegaciones de unos y otros Estados, de diferentes continentes y tradiciones jurídicas, son muy diversas y variadas. Tal disparidad se da incluso

sobre comercio electrónico brindándoles una legislación moderna, uniforme y cuidadosamente redactada para ellos, aludiendo a dos principios que han guiado toda la labor de la CNUDMI en materia de comercio electrónico: neutralidad tecnológica y equivalencia funcional[18].

1.1.1.1.3. Actividad de la CNUDMI/UNCITRAL posterior a la convención de Naciones Unidas sobre comunicaciones electrónicas

En su 40º período de sesiones, celebrado en 2007, la Comisión pidió a la Secretaría que siguiera de cerca la evolución legislativa en materia de comercio electrónico, con miras a efectuar, en su momento, sugerencias oportunas sobre la labor futura. En su 42º período de sesiones, celebrado en 2009, la Comisión pidió a la Secretaría que preparara un estudio sobre los documentos electrónicos transferibles, basándose en las propuestas presentadas en ese período de sesiones[19].

---

dentro de las distintas Delegaciones de los países miembros de la Unión Europea, a pesar de los intentos de mantener una posición común, al menos, en las cuestiones fundamentales objeto de debate. La gran dificultad, ya desde el primer artículo que se ocupe del ámbito de ampliación, radica en la naturaleza del objeto del proyecto de Convención. No se trata de una concreta institución jurídica, como pudiera ser una determinado contrato: compraventa, préstamo, garantía, etc. Se pretende regular en el ámbito internacional el uso de medios electrónicos en la contratación. Evidentemente el ámbito contractual es realmente amplio, y el régimen jurídico aplicable a cada particular contrato en cada ordenamiento jurídico resulta muy variado. Por esa razón la tarea no resulta fácil. Si se encuentran ámbitos de confluencia donde se pueda asumir un régimen jurídico común y uniforme, podrá existir una Convención que incentive y favorezca el desarrollo del comercio electrónico en el ámbito internacional". (MADRID PARRA, A.: Lento caminar hacia una posible convención sobre contratación electrónica", *Revista de la Contratación Electrónica*, núm. 49, 2004, págs.53-59).

[18] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 229. "Lo que se ha hecho ha sido proyectar sobre la base de la plantilla de la Convención de Viena los principios cardinales de la LMCE. El resultado ha sido la Convención sobre comunicaciones electrónicas, que no se circunscribe al contrato de compraventa, pero que pretende facilitar la aplicación de los principios rectores del comercio electrónico en la celebración y ejecución de los contratos internacionales en general".

[19] CNUDMI/UNCITRAL: *A/CN.9/681/Add.1 - Posible labor futura en materia de comercio electrónico: propuesta de los Estados Unidos de América sobre los documentos electrónicos transferibles*, Viena, 29 de junio a 17 de julio de 2009; CNUDMI/UNCITRAL: *A/CN.9/681/Add.2 - Posible labor futura en materia de comercio electrónico: propuesta de los Estados Unidos de América sobre la solución de controversias por vía informática*, Viena, 29 de junio a 17 de julio de 2009; y CNUDMI/UNCITRAL: *A/CN.9/682 - Propuesta de la Delegación Española para los trabajos futuros del Grupo de Trabajo IV de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*, Viena, 29 de junio a 17 de julio de 2009.

En el 45º período de sesiones[20] del Grupo de Trabajo IV (Comercio Electrónico) se inician las deliberaciones sobre las cuestiones jurídicas relativas al empleo de documentos electrónicos transferibles, instándose a los Estados miembros que faciliten información a fin de preparar documentos de trabajo para el siguiente periodo de sesiones.

El Grupo de Trabajo empezó por entablar un debate general sobre los documentos electrónicos transferibles[21]. De esta forma, se reconoce que, hasta el momento, no había ningún marco jurídico internacionalmente aceptado, generalizado y armonizado que regulara las diversas cuestiones que planteaban la utilización de documentos electrónicos transferibles, lo cual no incitaba a recurrir a ellos; pues, no podemos olvidar que la Convención sobre Comunicaciones Electrónicas en los Contratos Internacionales en su Artículo segundo los excluye de su ámbito de aplicación[22].

De esta forma, se muestra que muchas de las cuestiones jurídicas que se relacionan con ellos han sido tratadas y resueltas en normas nacionales e internacionales, faltando un grado suficiente de armonización a nivel transfronterizo que logre una mayor eficiencia en las operaciones, la financiación y el comercio a nivel internacional[23].

Asimismo, siendo conscientes de los interrogantes que se plantean, a la vez de los supuestos beneficios que puede conllevar que un instrumento trate este tema, el Grupo

[20] CNUDMI/UNCITRAL: *A/CN.9/737 - Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 45º período de sesiones*, Nueva York, 18 de junio a 6 de julio de 2012.

[21] CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.119 - Cuestiones jurídicas relativas al empleo de documentos electrónicos transferibles: propuesta de los Gobiernos de Colombia, España y los Estados Unidos*, Viena, 29 de octubre a 2 de noviembre de 2012, párr. 5, los define como: "Los documentos transferibles (es un término general que se refiere tanto a un título transferible (instrumentos financieros que pueden contener una promesa incondicional o una orden a un tercero de pagar una cantidad determinada de dinero al tenedor, por ejemplo lo que podría ser un crédito documentario) como a un documento de titularidad transferible (documentos que constituyen una prueba fehaciente de que el tenedor o el titular del documento tiene derecho a recibir, conservar y disponer de él y de las mercancías representadas en él, por ejemplo, una carta de embarque".

[22] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 80 y ss.

[23] CNUDMI/UNCITRAL: *A/CN.9/737 - Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 45º período de sesiones*, Nueva York, 18 de junio a 6 de julio de 2012, párr. 14; y CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.119 - Cuestiones jurídicas relativas al empleo de documentos electrónicos transferibles: propuesta de los Gobiernos de Colombia, España y los Estados Unidos*, Viena, 29 de octubre a 2 de noviembre de 2012, párr. 2.

de Trabajo alentó la consideración de esta cuestión como un posible tema de futuro[24], partiendo, de al menos, cinco principios básicos que son necesarios para los documentos electrónicos transferibles: a) la equivalencia electrónica de la escritura; b) la equivalencia electrónica de la firma electrónica; c) la unicidad y la garantía de singularidad; d) la transmisión de derechos; y, e) la identificación y la autenticación[25].

1.1.1.2. Conferencia de la Haya

La Conferencia de la Haya de Derecho Internacional Privado[26] es una organización intergubernamental de carácter mundial que elabora instrumentos jurídicos multilaterales que tratan de dar respuesta a las necesidades mundiales, al tiempo que garantiza su seguimiento, con el objetivo de promover la unificación progresiva de las normas de Derecho Internacional Privado.

El mandato estatutario de la Conferencia consiste en trabajar en pos de la unificación progresiva de estas normas. Ello implica encontrar enfoques reconocidos internacionalmente para cuestiones como la competencia de los tribunales, el Derecho aplicable, el reconocimiento y la ejecución de sentencias en numerosos ámbitos diferentes, desde el Derecho bancario o comercial hasta el procedimiento civil internacional.

Con el fin de armonizar la aplicación de los Convenios, la Secretaría organiza, ayuda y participa en conferencias y seminarios a nivel nacional e internacional

[24] Para el Grupo de Trabajo IV de la CNUDMI existen ejemplos de leyes nacionales que permiten el uso comercial satisfactorio de documentos electrónicos transferibles, pueden presentarse obstáculos jurídicos en el contexto transfronterizo (CNUDMI/UNCIRTRAL: *A/CN.9/WG.IV/WP.118 - Cuestiones jurídicas relativas al empleo de documentos electrónicos transferibles*, Viena, 29 de octubre a 2 de noviembre de 2012, párr. 27 y ss.

[25] En su último periodo de sesiones (50º sesión, Viena, 10 al 14 de noviembre de 2014), el Grupo de Trabajo IV de la CNUDMI prosiguió su labor de preparación del proyecto de disposiciones sobre documentos electrónicos transferibles. Asimismo se espera que el Grupo tome consideraciones de fondo (CNUDMI UNCITRAL: *A/CN.9/WG.IV/WP.129 - Programa provisional anotado*; *A/CN.9/WG.IV/WP.130 - Proyecto de disposiciones sobre los documentos electrónicos transferibles*; *A/CN.9/WG.IV/WP.130/Add.1 - Proyecto de disposiciones sobre los documentos electrónicos Transferibles*, Viena, 10 a 14 de noviembre de 2014.
Disponible en:
http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html (última visita: 9/12/2014).

[26] CONFERENCIA DE LA HAYA.
Disponible en: www.hcch.net (última visita: 31/5/2014).

orientados a la formación de las distintas personas implicadas en la aplicación de los Convenios, particularmente jueces, funcionarios de las Autoridades Centrales y juristas. Asimismo, se publica un boletín judicial sobre la protección internacional del niño. Diversos grupos de interesados, tales como parlamentarios o estudiantes, visitan con regularidad la Oficina Permanente. Un número creciente de pasantes y de funcionarios enviados por sus Gobiernos acuden en comisión de servicios a la Secretaría. Los miembros de la Oficina Permanente publican regularmente artículos en revistas especializadas y realizan aportaciones en libros y otras publicaciones.

1.1.1.2.1. Trabajos en materia de comercio electrónico

La Conferencia de La Haya de Derecho Internacional Privado ha organizado, desde finales de la década de los noventa, diversas conferencias y mesas redondas sobre comercio electrónico y derecho internacional privado a fin de analizar los múltiples aspectos que aquel representa y su incidencia en las normas.

Así, en septiembre de 1999, se celebró, en colaboración con la Universidad de Ginebra[27], una mesa redonda a fin de debatir sobre los problemas vinculados a la jurisdicción y a la ley aplicable al comercio electrónico y a las transacciones por Internet.

Durante la sesión se presentaron varios puntos destacados que defendían la importancia de Internet para el crecimiento económico. Así, se afirmó que Internet difiere de otras tecnologías en dos aspectos: en primer lugar, es inherentemente global, y en segundo lugar, se reduce enormemente las barreras económicas de entrada al comercio.

Como resultado, el número de proveedores de comercio electrónico, que aparecen en el mercado, aumenta drásticamente, a la vez que aumenta el número de empresas que aparecen en el mercado. Esto hace que las estrategias tradicionales de reglamentación

[27] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Geneva round table on Electronic Commerce and Private International Law*, Comunicado de prensa, septiembre de 1999. Disponible *en:* http://www.hcch.net/upload/wop/press01e.html (última visita: 31/5/2014).

para proteger a los consumidores y otros valores sociales sea cada vez más importante. Las recomendaciones de la mesa redonda se pueden sintetizar en lo siguiente:

a) En lugar de la creación de nuevas normas para el comercio electrónico y operaciones de internet, deben aplicarse los principios, reglas y procedimientos existentes, incluyendo el uso de equivalentes funcionales. De esta forma, se considera necesaria la aplicación de los principios establecidos en la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

b) Las normas deben ser, necesariamente, tecnológicamente neutrales.

c) Para los contratos en línea, en materia de jurisdicción y la ley aplicable, si el cumplimiento de la obligación correspondiente se lleva a cabo fuera de línea, las normas existentes de derecho internacional privado, que se refieren al lugar de actuación, siguen siendo pertinentes. Si la ejecución se realice en línea, el lugar de cumplimiento no es adecuado como factor de conexión. En ese caso, los factores de conexión relevantes son la ubicación de cada una de las partes involucradas.

d) En las transacciones electrónicas de negocio a negocio, la autonomía de las partes debe ser el principio rector, tanto en lo que respecta a la ley aplicable como a la jurisdicción.

e) Para las transacciones entre empresas y consumidores, se requiere otra evaluación a la luz de todos los intereses en juego. En particular, para evitar la dicotomía tradicional entre el "país de origen" (la del vendedor o proveedor) y el "país de acogida" (la del consumidor), se propuso comenzar un proceso de certificación en la línea de los trabajos realizados dentro de la Corte Penal Internacional y otras organizaciones privadas. Este proceso de certificación debía incluir reglas mínimas sustantivas de protección para el consumidor, incluyendo garantías, y un mecanismo de resolución de conflictos justa y fácil, que podría ser gratuito para el consumidor. Si un sitio no ha sido certificado, entonces la ley y los tribunales del lugar de origen son competentes, en caso contrario se podría aplicar la ley y los tribunales del lugar donde se encuentre el consumidor serían.

f) La identificación de los consumidores a través de la red es esencial para el buen funcionamiento del comercio electrónico.

g) En materia de protección de datos, la mesa redonda reconoció que la recopilación de datos incluidos los datos personales y su procesamiento son inherentes al comercio electrónico.

h) En materia de seguridad de los sistemas (confidencialidad, integridad, autenticación, no repudio y disponibilidad), se llegó a la conclusión de que la necesidad de confidencialidad no debe ser considerada como un impedimento para el uso de los formularios electrónicos de transmisión. Las técnicas actualmente existen para proteger la confidencialidad. Se sugirió que los Estados deben fomentar el uso de esas técnicas.

i) Por último, la Mesa Redonda consideró necesario el fomentado el desarrollo de mecanismos de resolución de conflictos en línea.

En marzo de 2000 se celebró, en Ottawa, una reunión de expertos bajo los auspicios de esta organización con el fin de evaluar las diversas cuestiones que se plantean en el comercio electrónico en relación con la competencia jurisdiccional internacional. Señalaron tres cuestiones esenciales: a) la distinción entre contratos celebrados en línea pero ejecutados fuera de ella y aquellos concluidos y ejecutados por vía electrónica; b) la identificación y la localización de las partes contratantes; y c) la irrelevancia de la tradicional distinción entre bienes y servicios en el comercio electrónico[28].

En octubre de 2004, la Conferencia de La Haya de Derecho Internacional Privado, la Cámara Internacional de Comercio y el Ministerio holandés de Asuntos Económico organizaron una "Conferencia Internacional sobre los aspectos jurídicos de una transacción de comercio electrónico", cuya actividad se centró en el desarrollo de la compraventa de bienes en línea en todas sus fases: precontractual, la celebración del contrato, su ejecución, y la fase post-contractual. Asimismo se trataron los distintos

[28] FEDELSTEIN DE CARDENAS, S. L.; SCOTI, L. B.: "El comercio electrónico en los foros de codificación internacionales: Conferencia de la Haya y las e-Apostillas", en *Contratación electrónica internacional: una mirada desde el derecho internacional privado* (Dir. Fedelstein de Cárdenas), Buenos Aires, 2008, pág. 92.

problemas jurídicos específicos que se plantean en el uso de los medios electrónicos de comunicación en cada una de las fases mencionadas[29].

1.1.1.2.2. Las e-Apostillas

El 5 de Octubre de 1961 se firmó el Convenio XII de la Conferencia de la Haya de Derecho Internacional Privado[30], por el que se suprimió la exigencia de legalización de los documentos públicos autorizados en el territorio de un Estado contratante y que deberían ser presentados en el territorio de otro Estado contratante, creando la Apostilla.

La Apostilla[31] es un trámite de legalización único, que consiste en colocar, sobre un documento público, una apostilla que certifica la autenticidad del documento expedido en otro país, suprimiendo las exigencias de legalización diplomática o consular para los documentos público, así lo dispone el Artículo 7 del Convenio[32].

Hoy en día, todo se vincula a temas electrónicos de forma que las nuevas tecnologías forman parte de la sociedad actual y su utilización es un hecho incontestable. De esta forma, la Comisión Especial sobre el funcionamiento práctico de los convenios sobre la Apostilla, la obtención de pruebas y la notificación, en el

[29] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO; CÁMARA INTERNACIONAL DE COMERCIO; MINISTERIO HOLANDÉS DE ASUNTOS ECONÓMICO INTERNATIONAL: *Conference on the Legal Aspects of an E-Commerce Transaction*, 26 y 27 octubre de 2004.
Disponible en: http://www.hcch.net/upload/wop/e-comm_intro_e.html (última visita: 31/5/2014).

[30] CONVENIO SUPRIMIENDO LA EXIGENCIA DE LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.
Disponible en: http://www.hcch.net/index_es.php?act=conventions.text&cid=41 (última visita:31/5/2014)

[31] MINISTERIO DE JUSTICIA DE ESPAÑA:
Disponible en:
http://www.mjusticia.gob.es/cs/Satellite/es/1200666550200/Tramite_C/1215326297910/Detalle.html (última visita: 31/5/2014).

[32] Artículo 7 del Convenio de la Conferencia de la Haya, nos dice: "Cada una de las autoridades designadas conforme al artículo 6 deberá llevar un registro o fichero en el que queden anotadas las Apostillas expedidas, indicando:

a) El número de orden y la fecha de la apostilla.
b) El nombre del signatario del documento público y la calidad en que haya actuado o, para los documentos no firmados, la indicación de la autoridad que haya puesto el sello o timbre.

A instancias de cualquier interesado, la autoridad que haya expedido la Apostilla deberá comprobar si las anotaciones incluidas en la Apostilla se ajustan a la del registro o fichero". (Texto íntegro del Convenio disponible en: http://www.hcch.net/index_es.php?act=conventions.text&cid=41).

establecimiento de una serie de conclusiones y recomendaciones[33], insistió en que la implantación de la nuevas tecnologías de la información "pueden tener efectos positivos en el funcionamiento del Convenio, de forma señalada en la disminución de los costes y en la mayor eficacia de los procedimientos de expedición y registro de apostillas".

Así, en virtud del Artículo 3 del Convenio, el efecto de una apostilla es "certificar la autenticidad de la firma, el carácter con el que ha actuado en signatario del documento, y en su caso, la identidad del sello o del timbre que lleva el documento", se recomienda a los Estados partes a que trabajen en el desarrollo de técnicas para generar apostillas electrónicas teniendo presentes la Ley Modelo de Comercio Electrónico y la Ley Modelo de Firma Electrónica, recogiendo los principios sobre los que versa, principalmente, la no discriminación y la equivalencia funcional.

En este contexto, la Conferencia de La Haya de Derecho Internacional Privado en abril de 2006, lanza el *e-Apostille Pilot Program* (e-APP)[34], que prevé: por una parte, la utilización de la tecnología en las Apostillas; por otra, se trabaja en la creación de registros electrónicos firmados por autoridades públicas.

Con la Apostilla electrónica se pretende ofrecer una mayor seguridad jurídica en el tráfico internacional, permitiendo agilizar los trámites para la expedición, así como, mejorar y fortalecer el servicio público que las administraciones brindan al ciudadano mediante la emisión de Apostillas y, al mismo tiempo, reducir las posibilidades de fraude. Dadas las ventajas del sistema de emisión de apostillas electrónicas la experiencia acumulada por los Estados pioneros, como por ejemplo España, resulta una coyuntura excepcional para fomentar la adopción de este sistema electrónico, dentro del ámbito del Convenio de la Haya de 1961 sobre la Apostilla.

---

[33] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Conclusiones y Recomendaciones adoptadas por la Comisión Especial sobre el Funcionamiento práctico de los Convenios sobre Apostilla, la Obtención de Pruebas y la Notificación.,* octubre/noviembre de 2003, párr.7.
Disponible en: http://www.hcch.net/index_es.php?act=publications.details&pid=3121&dtid=2 (última visita: 31/5/2014).

[34] Nueva Zelanda, el 13 de mayo de 2009, ha emitido la primera apostilla electrónica de conformidad con el modelo sugerido en virtud del Programa Piloto de Apostillas electrónicas, siendo la primera emitida en la región de Asía – Pacífico.

1.1.2. Ámbito regional

1.1.2.1. Asociación Económica de Asia y el Pacífico (APEC)

La APEC[35] fue fundada en 1989 y cuenta con 21 miembros[36], entre ellos todas las grandes economías de Asia y el Pacífico. Comenzó como un grupo informal de diálogo. Hoy, APEC se ha convertido en el vehículo primario regional para promover el comercio abierto y la cooperación económica. Los 21 miembros de la APEC representan aproximadamente el 42 por ciento de la población mundial y cerca del 49 por ciento del comercio mundial. La APEC tiene una Secretaría General, con sede en Singapur, encargada de coordinar el apoyo técnico y de consultoría. La APEC no tiene un tratado formal y, por ello, sus decisiones se toman por consenso, funcionando en base a declaraciones de carácter no vinculantes.

En materia de comercio electrónico, la APEC cuenta con el *Electronic Commerce Steering Group*[37] que tiene como función promover el desarrollo y la utilización del comercio electrónico mediante la creación de marcos legales, regulatorios y de política en la región de APEC de forma transparente y coherente. De esta forma, realiza una función de coordinación en la APEC en las actividades de comercio electrónico, basándose en principios establecidos internacionalmente. Asimismo, explora cómo las economías pueden desarrollar mejor un entorno legal, con políticas transparentes y optimizadas para permitir que las economías puedan utilizar las tecnologías de información y comunicación (TICs) y, así, poder impulsar el crecimiento económico y el desarrollo social de los Estados miembros. En este contexto, se trata de generar seguridad en las operaciones de comercio electrónico y promover así una infraestructura de clave pública normalizada e interoperativa[38].

---

[35] ASOCIACIÓN ECONÓMICA DE ASIA Y EL PACÍFICO (APEC).
Disponible en: http://www.apec.org/ (última visita: 31/5/2014).

[36] Australia, Brunei, Canadá, Chile, China, Hong Kong (China), Indonesia, Japón, Corea, Malasia, México, Nueva Zelanda, Papua Nueva Guinea, Perú, Filipinas, Rusia, Singapur, Taipei, Tailandia, Estados Unidos y Vietnam.

[37] ELECTRONIC COMMERCE STEERING GROUP:
Disponible en: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx (última visita: 31/5/2014).

[38] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.153.

La APEC, a través de este Grupo, ha realizado un conjunto iniciativas con el fin de ayudar a los Estados miembros a poder aprovechar los desarrollos del comercio electrónico. Así, en el año 2000 se lanzó el denominado *Action Agenda for the New Economy*[39], que tiene por objeto promover un "ambiente político adecuado" y proporcionar un marco que pueda ayudar a fortalecer los mercados de cara al comercio electrónico en cuanto a su infraestructura, su conocimientos y el desarrollo de las habilidades de todos los Estados miembros. Todo ello, se hace con el objeto de trabajar para proveer un "acceso asequible y seguro a los servicios de Internet". La estrategia electrónica de la APEC fue aprobada en 2001[40]. Se trata de un plan orientado a largo plazo basado en fundamentalmente en tres pilares:

a) Crear un entorno para el fortalecimiento de las estructuras e instituciones del mercado. Se insta a las economías a implementar políticas y medidas adecuadas para promover un crecimiento sostenible a través de un marco de política macroeconómica, un régimen de competencia efectiva, una buena gestión financiera y empresarial, eficiencia de los mercados de capital de riesgo, un sólido marco jurídico de la propiedad intelectual, gestión del riesgo, toma de decisiones transparente, fuertes marcos institucionales, flexible mercados laborales y políticas sociales focalizadas. En su ausencia, la evolución de la nueva economía podría elevar el costo a los gobiernos.

b) Facilitar un ambiente para la inversión en infraestructura y desarrollo tecnológico: un marco legal normativo proporciona el fundamento esencial para el crecimiento de la inversión empresarial y la confianza de los consumidores; las leyes proporcionan una labor esencial en la autenticación de las transacción y, a través de las firmas electrónicas, proporcionan la

[39] APEC: *APEC Economic Leaders' Declaration: Delivering to the Community. Annex 1 - Action Agenda for New Economy*, Brunei, 16 de noviembre 2000.
Disponible en:
http://www.apec.org/Meeting-Papers/Leaders-Declarations/2000/2000_aelm/annex1_action_agenda.aspx (última vista: 31/5/2014).

[40] APEC: *2001 Leaders' Declaration: Shanghai Declaration - Meeting New Challenges in the New Century (Action Agenda for the New Economy). Appendix 2 - e-APEC Strategy*, Shanghai, China, 21 de octubre 2001.
Disponible en:
http://www.apec.org/Meeting-Papers/Leaders-Declarations/2001/2001_aelm/appendix2_eAPEC_strategy.aspx (última visita:31/5/2014).

seguridad de la información, la protección de datos personales y la confianza del consumidor.

c) Mejorar la capacidad humana y promover el espíritu empresarial, instando a tomar medidas para mejorar la mencionada capacitación de las personas y fomentar el espíritu empresarial. Es de vital importancia mejorar la capacidad humana para establecer una posición ganadora en la nueva economía. El espíritu empresarial es fundamental para generar nuevas ideas y desarrollar nuevas oportunidades de negocio. Así, se hace una llamada de atención al fortalecimiento de la cooperación tecnológica y de la información, además de existir la necesidad de acelerar la implantación de la economía digital.

1.1.2.2. MERCOSUR

El 26 de marzo de 1991 se firmó, en Asunción, el Tratado constitutivo del Mercado Común del Sur (MERCOSUR[41]) en el que Argentina, Brasil, Paraguay y Uruguay sentaron las bases para la creación de un mercado común, estableciendo en su Artículo 1º los medios para la consecución de este objetivo, garantizando las libertades de circulación de mercancías, de personas, de servicios y de capitales.

La libre circulación implica un intercambio fluido entre los Estados partes que precisa de la armonización de las leyes en determinadas áreas claves, a la vez que requiere la supresión de fronteras para permitir la libre circulación de personas, capitales, bienes y servicios[42]. Tal como se estipula en el Artículo 1º en su parte final se requiere "el compromiso de los Estados Partes de armonizar sus legislaciones, en las áreas pertinentes, para lograr el fortalecimiento del proceso de integración". De esta forma, surge la necesidad de cumplir los propósitos recogidos en el Tratado, lo que

[41] MERCOSUR:
Disponible en: http://www.mercosur.int/ (última visita: 31/5/2014).

[42] FELDESTEIN DE CARDENAS, S. L.: "El Derecho Internacional Privado y los procesos de integración regional", *Revista Forense del temas de Derecho Privado,* Buenos Aires, 2000, págs. 199 y ss.

lleva a hacer de las leyes instrumentos funcionales y ágiles destinadas a facilitar y reglar las relaciones que se anudan dentro del ámbito MERCOSUR.

MERCOSUR trabaja por una mayor inserción competitiva mundial por medio de la ampliación de sus mercados internos y la modernización de las economías nacionales. Por ello, el Tratado de Asunción hizo explícita la necesidad de promover el desarrollo científico y tecnológico de los Estados parte, además de ampliar la oferta y calidad de los bienes y servicios disponibles, a fin de mejorar las condiciones de vida de sus habitantes[43]. Por ello, el comercio electrónico, en particular la contratación electrónica regional, es una de esas áreas, que en los términos del Artículo 1º del Tratado, en las que hay que procurar armonizar.

En el marco de MERCOSUR el órgano competente en materia de comercio electrónico es el Subgrupo de Trabajo Nº 13 (SGT 13)[44], dependiente del Grupo de Comercio Común.

Por otro lado, debemos hacer referencia a la Reunión Especializada de Ciencia y Tecnología (RECyT)[45] del MERCOSUR, creada en 1992, sugerida por los presidentes de los Estados parte durante la segunda reunión del Consejo Mercado Común. Tiene como objetivo central la promoción y el desarrollo científico y tecnológico de los Países Miembro del MERCOSUR así como modernizar sus economías para ampliar la oferta y la calidad de los bienes y servicios disponibles, a fin de mejorar las condiciones de vida de sus habitantes. Sus acciones están estructuradas en el sentido de aumentar la productividad de las economías del MERCOSUR y ampliar la competitividad de los segmentos productivos del MERCOSUR en terceros mercados.

---

[43] FELDESTEIN DE CARDENAS, S. L. y BEATRIZ SCOTTI, L.: "La Convención sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales: un avance hacia la armonización legislativa en materia de contratación electrónica" en *Contratación electrónica internacional: una mirada desde el Derecho Internacional Privado* (Dir. Feldestein de Cardenas, S. L.; Coords. Andrea Medina, F.; Sofia Rodríguez, M.; y, Beatriz Scotti, L.), Buenos Aires, 2008, págs.78 y ss.

[44] ESTRUCTURA INSTITUCIONAL DEL MERCOSUR: Subgrupo de Trabajo Nº 13 MERCOSUR Disponible en: http://www.mercosur.int/innovaportal/v/273/1/secretaria/estructura_institucional_del_mercosur (última visita: 31/5/2014).

[45] REUNIÓN ESPECIALIZADA DE CIENCIA Y TECNOLOGÍA (RECYT) DEL MERCOSUR. Disponible: http://www.recyt.mincyt.gov.ar/ (última visita: 31/5/2014).

En este contexto se trabaja en un proyecto denominado: MERCOSUR DIGITAL. Se trata de un proyecto de cooperación internacional entre la Unión Europea y MERCOSUR, que tiene como objetivo de reducir las asimetrías legales y tecnológicas entre ambas regiones. Además, busca promover políticas y estrategias comunes en el área de la Sociedad de la Información que contribuyan al crecimiento, la integración económica y el desarrollo del comercio electrónico de los países miembros[46].

MERCOSUR DIGITAL fue concebido para promover la capacitación tecnológica en recursos especializados en TICs y crear las condiciones necesarias que permitan desarrollar un comercio electrónico eficaz, fortaleciendo la economía digital y trabajando por una simetría estructural entre los países. Tiene su enfoque principal en las áreas de comercio electrónico, formación continua de recursos humanos, desarrollo de las pequeñas y medianas empresas y temas de la Sociedad de la Información a partir de dos vertientes:

a) En lo que respecta al comercio electrónico, trabaja en la creación de un marco regulatorio común de infraestructura tecnológica en el MERCOSUR para temas referentes a la certificación digital, infraestructura de claves públicas, sello de tiempo, protección de datos para negociaciones transnacionales y desarrollo de una plataforma común para la venta de productos y servicios direccionados a las pequeñas y medianas empresas.

b) Y en lo que se refiere a la educación permanente, se trata de implantar una red de capacitación que integre a los países del bloque, aprovechando las capacidades y fortalezas institucionales ya existentes para incrementar competencias y conocimientos para la Sociedad de la Información de sectores públicos y privados.

[46]MERCOSUR DIGITAL:
Disponible en:
http://www.recyt.mincyt.gov.ar/index.php?option=com_content&view=article&id=385&Itemid=50&lang=es (última visita: 31/5/2014).

1.1.2.3. Unión Europea (UE)

El 13 de diciembre de 1999 fue aprobada la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica[47], pues como dice la propia Directiva en su Considerando cinco, "la comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico".

Con la Directiva se pretende instaurar un marco comunitario sobre condiciones aplicables a la firma electrónica de manera que aumente la confianza en las nuevas tecnologías y la aceptación general de las mismas. De esta forma, se trata de armonizar la legislación de los Estados miembros en este ámbito para no obstaculizar la libre circulación de bienes y servicios en el mercado interior; asimismo, se hace preciso promover la interoperabilidad de los productos de firma electrónica de conformidad con el Artículo 14 del Tratado; el mercado interior implica un espacio sin fronteras interiores, en el que esté garantizada la libre circulación de mercancías, debiendo satisfacer los requisitos esenciales de los productos de firma electrónica para fomentar la confianza en la citada firma electrónica.

Sin embargo, la Directiva sobre la firma electrónica si bien ha tenido como resultado un cierto grado de armonización en Europa, los Estados, en su transposición al derecho interno, han establecido marcos jurídicos distintos que hacen imposible en la práctica realizar transacciones electrónicas transfronterizas.

[47] DIRECTIVA 1999/93/CE:
Disponible en:
http://eur-lex.europa.eu/legal-content/ES/ALL/;jsessionid=Wt3bTHHXQvYQ3f97GNlZqL1Lk8mYS6MQQkpRKj5vx0m3k6Npqn60!-1917706091?uri=CELEX:31999L0093 (ultima vista: 31/5/2014).

De esta manera, la Comisión Europea[48], con el fin de facilitar las transacciones electrónicas transfronterizas seguras en Europa y, a la vez, evitar la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia[49], comenzó a trabajar[50] en un nuevo proyecto en forma de Reglamento[51] que prestara especial atención a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, con el fin de recoger garantías para que las personas y las empresas puedan usar sus propios sistemas de identificación electrónica nacionales en otros países de la UE en que exista la identificación electrónica. Este Reglamento[52] fue aprobado finalmente el 23 de julio de 2014.

El citado Reglamento[53] se presentó sobre la base de una propuesta emitida por la Comisión fundamentada en el Artículo 114 del TFUE, que se refiere a la adopción de

[48] COMISIÓN EUROPEA: *Agenda Digital: nuevo Reglamento para hacer posible la firma electrónica transfronteriza y sacar más ventaja de la identificación electrónica en el mercado único digital*, Comunicado de prensa, Bruselas, 4 de junio de 2012.
Disponible en: http://europa.eu/rapid/press-release_IP-12-558_es.htm (última visita: 31/5/2014).

[49] COMISIÓN EUROPEA: *Comunicación: Una Agenda Digital para Europa*, Bruselas, 26 de agosto de 2010, págs. 6 y ss.
Disponible: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245&from=es (última visita: 1/6/2014).

[50] Este trabajo vino impulsado también por: el Consejo Europeo invitó a la Comisión a contribuir al mercado único digital creando condiciones apropiadas para el reconocimiento mutuo a través de las fronteras de instrumentos clave tales como la identificación electrónica, los documentos electrónicos, las firmas electrónicas y los servicios de entrega electrónica, así como para unos servicios de administración electrónica interoperables en toda la Unión Europea. Por ello, se pide a la Comisión que elabore un plan de trabajo para que el mercado único digital esté plenamente implantado en 2015.; y que, además, informe en octubre de 2011 sobre estos sectores potenciadores de crecimiento (SECRETARÍA GENERAL DEL CONSEJO DE ESTADO: *Consejo Europeo 23 y 24 de junio de 2011: conclusiones*, Bruselas, 29 de septiembre de 2011, pág. 3.); y el Parlamento Europea que en su Resolución de 21 de septiembre de 2010 sobre la plena realización del mercado interior del comercio electrónico, pidió a la Comisión que estableciese una pasarela de autoridades europeas de validación a fin de garantizar la interoperabilidad transfronteriza de las firmas electrónicas y aumentar la seguridad de las transacciones realizadas a través de Internet (Considerando 7 del Reglamento Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior).

[51] Proyecto de Resolución legislativa del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%2BREPORT%2BA7-2013-0365%2B0%2BDOC%2BXML%2BV0//ES# (última visita: 31/5/2014).

[52] Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, publicado en el Diario Oficial de la Unión Europea el 28 de agosto de 2014.
Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910 (última visita: 2/10/2014).

[53] COMISIÓN EUROPEA: Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior COM (2012) 238 final, 2012/0146 (COD), Bruselas, 4 de junio de 2012.

normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. De esta manera, se considera que un Reglamento es el instrumento jurídico más apropiado. La aplicabilidad directa de un Reglamento en virtud del artículo 288 del TFUE reducirá la fragmentación jurídica y aportará mayor seguridad jurídica

Con este Reglamento se viene a plantear un mercado único de la firma electrónica y los servicios de confianza en línea afines más allá de las fronteras, asegurando que esos servicios funcionen y gocen del mismo estatuto jurídico que los trámites tradicionales en papel, dándose pleno efecto a los posibles ahorros propiciados por la contratación electrónica. Por otro lado, se pretende respetar los sistemas de identificación nacionales, así como las preferencias de los Estados miembros que no tienen sistemas nacionales de identificación, permitiendo a los países que si tienen sistemas de identificación electrónica optar por quedar fuera del sistema paneuropeo. Si un Estado miembro notifica que desea sumarse a este sistema deberá ofrecer el mismo acceso a los servicios públicos mediante la identificación electrónica que a sus propios ciudadanos. Así, se trata de dar un reconocimiento recíproco a las identificaciones electrónicas nacionales, a la vez que se quiere establecer normas comunes sobre los servicios de confianza y la firma electrónica. De esta forma, se pretende profundizar en la mejorara la legislación existente y en la ampliación del reconocimiento y la aceptación mutua, dentro de la Unión Europea, de los sistemas de identificación electrónica y otros servicios de confianza electrónicos conexos.

1.2. Plano estatal

1.2.1. Australia

En 1996, tras la aprobación de la Ley Modelo sobre Comercio electrónico, el Gobierno de Australia se dio cuenta de la necesidad de establecer un marco para el reconocimiento del comercio electrónico. Así, en 1997 creó la *National Office of the*

Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:ES:PDF (última visita: 31/5/2014).

Information Economy (NOIE)[54], con el objeto de promover y coordinar estrategias para la utilización de las nuevas tecnologías de la información y ofrecer políticas estandarizadas. Como parte de estrategia, se creó el *Electronic Commerce Expert Group* (ECEG)[55], formado por representantes de las empresas más importantes del país, profesionales del derecho y miembros del Gobierno de Australia, para examinar los obstáculos legales existentes para el desarrollo del comercio electrónico en el país.

Este Grupo de Expertos, tras examinar las cuestiones jurídicas y la forma más apropiada para su regulación, en consonancia con la evolución internacional, para hacer frente a esas cuestiones, el 31 de marzo de 1998, elaboró un informe[56] con el fin de promulgar una Ley basada Ley Modelo sobre Comercio Electrónico, elaborada por la CNUDMI, con algunas modificaciones.

El informe de la ECEG, contenía unas recomendaciones en las que se identificaba la importancia de adherirse a los principios de la Ley Modelo para garantizar un enfoque coordinado a nivel internacional. De esta manera, recomendó que se optara por una ley marco a partir de la cual se adoptaran las demás leyes de los distintos Estados de Australia[57]. Igualmente, recomendó que se abarcarán temas como: las comunicaciones en el comercio electrónico en sentido amplio; un enfoque genérico con la firma electrónica (sin prescripción tecnológica), cuidadosa en las excepciones; equivalencia funcional, en referencia a los requisitos legales de la escritura, firma y la originalidad; una disposición relativa a los mensajes de datos utilizados en la formación del contrato, etc.[58].

---

[54] National Office of the Information Economy (NOIE) ha sido sustituida por la Australian Government Information Management Office (AGIMO), asumiendo las funciones de la anterior.
Disponible en: http://www.noie.gov.au/ (última visita (6/6/2014).

[55] LOW, R.; CHRISTENSEN, S.: "Electronic signatures and PKI frameworks in Australia", *Digital Evidence and Electronic Signature Law Review*, núm.1, octubre, 2004.

[56] ELECTRONIC COMMERCE EXPERT GROUP TO THE ATTORNEY GENERAL: *Electronic Commerce: Building the Legal Framework*, 31 de marzo de 1998.
Disponible en: http://catalogue.nla.gov.au/Record/337366 (última visita: 6/6/2014).

[57] Teniendo en cuenta que Australia es una Federación, compuesta de 6 Estados y varios territorios, que se denominan formalmente Commonwealth de Australia.

[58] UPCROFT, A.: "E-Commerce: Global or Local? An Australian Case Study", *Journal of Law, Information and Science*, 1999, núm.113.
Disponible en: http://www.austlii.edu.au/au/journals/JlLawInfoSci/1999/5.html#Heading11 (última visita: 6/6/2014).

En este contexto, el 30 de junio de 1999 fue aprobada la *Electronic Transactions Act*[59], que tenía como objetivo primordial establecer una marco normativo que reconociese la importancia de la economía de la información, para la futura prosperidad económica y social de Australia; facilitar el uso de las transacciones electrónicas; promover la confianza de las empresas y la comunidad en el uso de las transacciones electrónicas; y permitir a las empresas y a la comunidad australiana utilizar las comunicaciones electrónicas en sus relaciones con el gobierno. La Ley ha sido descrita como una "ley de estilo de interpretación", cuyo propósito central es establecer que las comunicaciones electrónicas pueden satisfacer los requisitos de las Leyes promulgadas por los demás Estados de la Commonwealth de Australia, en relación con la escritura, la firma, la presentación de documentos originales y el almacenamiento electrónico de datos.

Esta Ley fue modificada en 2011 con el fin de incluir disposiciones sustantivas de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[60].

Es importante destacar que, en el desarrollo de un enfoque uniforme para el comercio electrónico, Australia ha participado en distintas formas de acuerdos con otros países. Estos acuerdos son indicativos de la actitud comprometida de Australia para promover el fomento del comercio electrónico mundial. Entre ellos destaca: por un lado, un Acuerdo Bilateral entre Australia y Estados Unidos[61], realizado a finales de 1998, sobre el comercio electrónico, que viene a confirmar un enfoque coordinado en las áreas claves del comercio electrónico entre los dos países. Esto incluye la estrecha cooperación en foros internacionales para promover el comercio electrónico mundial y facilitar un marco legal transparente y coherente; y, por otro lado, un Memorando de Entendimiento entre Australia, Singapur, Malasia, República de Indonesia, Brunei,

[59] AUSTRALIA: Electronic Transactions Act (Act No. 162 of 1999 as amended, taking into account amendments up to Electronic Transactions Amendment Act 2011).
Disponible en: http://www.comlaw.gov.au/Details/C2011C00445/Html/Text#_Toc296406945 (última visita:6/6/2014).

[60] Situación actual de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). Disponible en: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model_status.html (última vista) .

[61] THE WHITE HOUSE (Office of the Press Secretary): *Joint Statement from Australia and the United States on electronic commerce*, 30 de noviembre 1998.
Disponible en: http://www.peterswire.net/privarchives/1998-11-30-joint-statement-with-australia-on-electronic-commerce.html (última visita: 6/6/2014).

Filipinas y Tailandia[62], celebrado el 27 de julio de de 1999, consistente en un entendimiento en materia de tecnología de la información. Los términos de este acuerdo incluyen la cooperación en cuestiones de comercio electrónico.

1.2.2. Estados Unidos

En Estados Unidos, a comienzos de los años 90, multitud de Estados de la Unión se dotaron de legislaciones en materia de firma electrónica, lo que provocó la preocupación de los juristas del país, ya que esto podría incitar la existencia de regulaciones dispares[63]. Mientras el Congreso de los Estados Unidos consideraba la importancia del comercio electrónico y la adaptación del *Uniform Commercial Code* al ciberespacio, muchos eran los Estados los que se estaban dotando de legislación sobre firma electrónica.

El primero de los Estados en dotarse de una Ley en esta materia fue UTAH (*Utah Digital Signatura Act*) en 1996[64]. Esta Ley no era neutral tecnológicamente, sino que se basaba en tecnología PKI, equiparaba las firmas electrónicas a las firmas manuscritas y detallaba los derechos y responsabilidades de las partes de una transacción[65]. Otros Estados siguieron el ejemplo de UTAH, por ansiedad o por necesidad de no quedarse atrás en demostrar que podían dar una respuesta a las nuevas necesidades que se presentaban en el nuevo marco tecnológico. Con posterioridad a la Ley UTAH se unieron más de 40 Estados, adoptando leyes que reconocían oficialmente algún tipo de firma electrónica, entre ellos: Arizona, Florida, Hawai, Michigan, Nuevo México,

---

[62] ASEAN: *Memorandum of Understanding between the Governments of the Member Countries of the Association of Southeast Asia Nations and the Government of Australia on the ASEAN-Australia Economic Cooperation Programme (AAECP),* Bangkok, Thailand, 27 July 1999.
Disponible en: http://www.asean.org/communities/asean-economic-community/item/memorandum-of-understanding-concerning-cooperation-on-standards-and-conformance-between-the-governments-of-brunei-darussalam-the-republic-of-indonesia-malaysia-the-republic-of-the-philippines-the-republic-of-singapore-the-kingdom-of-thailand-and-the-socia (última visita: 3/6/2014).

[63] OREGA DÍAZ, J.F.*: La firma electrónica y el contrato de certificación electrónico*, Madrid, 2008, págs.76 y 77.

[64] Utah Digital Signature Act Utah. Code §§ 46-3-101 to 46-3-504. (Promulgada en 1995).
Disponible en: http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html (última visita: 31/5/2014).

[65] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma electrónica y autoridades de certificación*, Madrid, 2000, pág. 91.

Nueva York, etc.[66]. A esto hay que sumar que, en 1997, había países que ya se habían dotado de leyes sobre firma electrónica, como Alemania, Italia o Malasia, en esa necesidad de tomar impulso en la ventaja que se asegura ser el "primer motor".

Ante el problema que se planteaba, el 30 de julio de 2000, el Congreso Federal norteamericano aprobó la Ley de firma electrónica de Estados Unidos (*Electronic Signature in Global and Nacional Commerce Act*)[67], Ley que fue considerada, en su momento, por los medios de comunicación del país, como de gran importancia para los negocios en red, a la vez que resaltaban la poca repercusión que había tenido en Europa.

Esta Ley se promulgó con el fin de hacer frente a las incertidumbres que se habían provocado por las normas estatales. Por consiguiente, la Ley trata de establecer una situación de confianza proporcionando un marco jurídico para hacer cosas que hasta la fecha se podían hacer, pero que no se hacían. Así, la E-Sign, como se conoce a esta Ley de firma electrónica, ofrece una regla general de la validez de los documentos electrónicos y firmas para las transacciones que afecten al comercio interestatal e internacional, permitiendo el uso de registros electrónicos para satisfacer cualquier ley o reglamento que exija que tal información se facilitara por escrito[68].

La E-Sign se encuentra acompañado de la Ley Uniforme de Transacciones Electrónicas (*Uniform Electronic Transaction Act* – UETA) [69], Ley modelo aprobada y recomendada a los Estados de la Unión para su aprobación por la Conferencia Nacional de Comisionados sobre Leyes Estatales Uniformes en julio de 1999, diseñada para proveer a cada Estado de estándares para el uso de y aceptación de la firma electrónica.

---

[66] SCHWARTZ, J.: *Archives - E-Signatures Become Valid For Business*, noticia The New York Times, publicada, el 2 de octubre de 2000.
Disponible en: http://www.nytimes.com/2000/10/02/business/e-signatures-become-valid-for-business.html (última visita: 31/5/2014).

[67] ELECTRONIC SIGNATURE IN GLOBAL AND NACIONAL COMMERCE ACT (E-SIGN)
Disponible en: http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (última visita: 31/5/2014).

[68] OMB; DEPARTMENTS OF COMMERCE, JUSTICE, AND TREASURY: G*uidance on implementng the Electronic Signatures in Global and National Commerce Act (E-SIGN)*. (Este documento está destinado sólo para la gestión interna del gobierno federal. No establece interpretaciones jurídicamente vinculantes, normas o estándares. Las agencias deben realizar su propia línea de acción, respecto a la forma de abordar los temas tratados en este documento, en el contexto de sus programas).
Disponible en: http://csrc.nist.gov/drivers/documents/esign-guidance.pdf (última visita: 31/5/2014).

[69] UNIFORM ELECTRONIC TRANSACTION ACT (UETA):
http://www.alabama.gov/PDFs/egov_pdfs/e-govUETA.pdf (última visita: 1/6/2014).

La E-Sign Act es una Ley de superposición, es decir, una Ley que se superpone a las leyes federales y estatales, que da fuerza y efecto legal a las firmas electrónicas y registros electrónicos[70], en lugar de establecer un protocolo tecnológico específico, por lo que las partes involucradas en la transacción deberán pactar la tecnología y la seguridad que consideren oportuna.

1.2.3. Singapur

En julio de 1998, se promulgó en Singapur la *Electronic Transaction Act*[71], con el objetivo de proporcionar una base legal en materia de derecho y obligaciones a las partes que participan en las transacciones electrónicas, a la vez que pretendía abordar los problemas que podrían surgir en el comercio electrónico. De esta forma, se intentan eliminar las barreras existentes a la hora de desarrollar el comercio electrónico que nacían de la incertidumbre de la escritura y los requisitos de firma, promoviendo la infraestructura necesaria para dar seguridad a las transacciones electrónicas.

Tras la promulgación de la ley se produjo una gran proliferación de bienes y servicios proporcionados en línea por organismo públicos y privados, que llevó a plantearse si la regulación existente era suficiente a fin de mantener firme un mercado en constante evolución.

El 6 de julio de 2006, Singapur firmó la Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[72], adoptado por la Asamblea General de la CNUDMI el 23 de noviembre de 2005. El 7 de julio de 2010 ratificó el Convenio para su entrada en vigor el 1 de marzo de 2013[73].

---

[70] WALKER, E. F.: *Practical Guide to E-Sign and Uniform Electronic Transaction Act*, 2002, pág. 1 y ss.
[71] SINGAPUR: Electronic Transactions Act (1998)
Disponible en: http://gcis.nat.gov.tw/eclaw/english/PDF/ElectronicTransactionsAct1998.pdf (última visita: 31/5/2014).
[72] UN DEPARTMENT OF PUBLIC INFORMATION: Press Release. China, Singapore, Sri Lanka sign un Convention on Use of Electronic Communications in International Contracts, Nueva York, 6 de Julio de 2006.
Disponible en: http://www.un.org/News/Press/docs/2006/lt4396.doc.htm (última visita: 31/5/2014).
[73] Situación actual Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005)
Disponible en:
http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention_status.html (última visita: 31/5/2014).

Con la firma de la Convención, surgió la necesidad de incorporar al ordenamiento jurídico interno la legislación existente en el contexto internacional, modificando la Ley de 1998 con el fin de adaptarla a los problemas que se venían planteando. Así pues, se realiza una revisión pública por parte de la *Info-Communications Development Authority of Singapore* (IDA)[74] y la *Attorney-General's Chambers* (AGC), en consulta con distintos los Ministerios. En las reuniones celebradas se desarrollaron una serie de recomendaciones que terminaron consolidándose en un informe que tiene por título *Joint IDA-AGC: Review of Electronic Transactions Act Proposed Amendments 2009* (Report)", emitido el 30 de junio de 2009[75].

Fruto de este informe fue la nueva Electronic Transaction Act[76], aprobada el 19 de mayo de 2010, que tiene como fin derogar su antecesora, la Ley de Transacciones Electrónicas de 1998, y como principal objetivo adaptar el marco jurídico de Singapur a la mencionada Convención, al mismo tiempo trata de facilitar la prestación de servicios de administración electrónica y adoptar un marco de acreditación para la regulación de las entidades emisoras de certificados.

1.2.4. China

La primera regulación en materia electrónica en China se encuentra en la Ley de Contratos de 1999[77], que en su Artículo 11 reconocía el mensaje de datos como equivalente a la forma escrita[78], a la vez que en su Artículo 16 se hacía referencia al

[74] INFO-COMMUNICATIONS DEVELOPMENT AUTHORITY OF SINGAPORE (IDA)
Disponible en: http://www.ida.gov.sg/ (última visita: 31/5/2014).
[75] IDA; AGC: *Joint IDA-AGC Review of Electronic Transactions Act: Proposed Amendments 2009*.
Disponible en:
http://www.ida.gov.sg/Policies-and-Regulations/Consultation-Papers-and-Decisions/Store/Joint-IDA-AGC-Review-of-Electronic-Transactions-Act-Proposed-Amendments-2009 (última visita: 31/5/2014)
[76] SINGAPUR: Electronic Transactions Act (2010 - Cap. 88).
Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN040992.pdf (última visita: 31/5/2014). (También disponible a través de: http://statutes.agc.gov.sg/aol/home.w3p).
[77] CHINA: Contract Law of the People's Republic of China (Adoptada y promulgada el 15 de marzo 1999).
Disponible en: http://www.novexcn.com/contract_law_99.html (última visita: 31/5/2014).
[78] Artículo 11 dice: "Definition of Writing: A writing means a memorandum of contract, letter or electronic message (including telegram, telex, facsimile, electronic data exchange and electronic mail), etc. which is capable of expressing its contents in a tangible form".

momento en que se formaba el contrato[79] y en su Artículo 34 se relacionaba el lugar en el que se formalizaba el contrato[80]. Esta Ley fue muy criticada, pues sólo reconocía el mensaje de datos como una forma de escritura, lo que limitaba sus funciones, ya que no se prescribía nada sobre su admisibilidad como prueba ante los tribunales, la originalidad, etc.[81].

A comienzos del año 2000, se empiezan a promulgar normas, a nivel provincial, con el fin de regular las transacciones electrónicas tales como la provincia de Hanain que adopta la *Hainan Administrative Measures on Digital Certification* en 2001, Shangai también aprobó la *Shanghai Administrative Measure on Digital Certificates* el 18 Noviembre de 2002, o la provincial de Guangdong aprobó la *The Electronic Transactions Regulations* el 6 de diciembre de 2003. Estas normas eran muy divergentes y se referían, sobre todo, a la seguridad y administración de la información, la infraestructura del sistema, etc. dejando de lado cuestiones esenciales como la firma electrónica, la protección del consumidor o la responsabilidad.[82]

Ante esta situación, teniendo en cuenta la importancia del comercio electrónico y su rápido desarrollo a nivel internacional, surgió la necesidad de aclarar la validez legal y seguridad de los documentos electrónicos, a la vez que se hizo vital la regulación efectiva de los prestadores de servicios de certificación.

De esta forma, el 28 de agosto de 2004, la Asamblea Popular Nacional de China aprobó la Ley de Firmas Electrónicas de la República Popular de China, que entró en

[79] Artículo 16 dice: "Effectiveness of Offer, Offer through Electronic Message: An offer becomes effective when it reaches the offeree. When a contract is concluded by the exchange of electronic messages, if the recipient of an electronic message has designated a specific system to receive it, the time when the electronic message enters into such specific system is deemed its time of arrival; if no specific system has been designated, the time when the electronic message first enters into any of the recipient's systems is deemed its time of arrival".

[80] Artículo 34 dice: "Place of Formation: Electronic Messages The place where the acceptance becomes effective is the place of formation of a contract. Where a contract is concluded by the exchange of electronic messages, the recipient's main place of business is the place of formation of the contract; if the recipient does not have a main place of business, its habitual residence is the place of formation of the contract. If the parties have agreed otherwise, such agreement prevails".

[81] MINYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *Science Direct Review*, enero, 2007, págs. 32 – 41.

[82] BLYTHE, S.E.: "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce", *Chicago-Kent Journal of Intellectual Property*, vol. 7, núm.1, 2007, págs.1-32.
Disponible en: http://scholarship.kentlaw.iit.edu/ckjip/vol7/iss1/ (última visita: 31/5/2014).

vigor el 1 de abril de 2005[83], con el fin de estandarizar los actos de firma electrónica, validación de los efectos jurídicos de la firma electrónica, y salvaguardar los derechos e intereses legítimos de las partes interesadas. Y lo hacen partiendo de: las Leyes Modelo sobre Comercio Electrónico y Firma Electrónica, las Directivas europeas sobre Comercio Electrónico y Firma Electrónica, la *E-Sign* de Estados Unidos y, muy especialmente, la *Electronic Transactions Act de Singapur*. Como complemento a esta Ley se aprobó por el Ministerio de Industria de la Información el Reglamento de la Autoridad de Certificación, que entró en vigor el 1 de abril de 2005.[84]

China firmó la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005, el 6 de julio de 2006[85], junto a Singapur y Sri Lanka; no obstante, aún no se ha pronunciado sobre su ratificación[86].

1.2.5. Argentina

Argentina muestra en su legislación una corriente que le acerca a Europa, algo que se muestra actualmente con el proyecto de MERCOSUR Digital, tal y como hemos explicado anterioriormente.

En 2001 aprobó la Ley 25.506 sobre Documento Electrónico y Firma Digital[87], que viene a crear una nueva forma de interactuar entre las personas físicas y jurídicas, y entre éstas y la Administración Pública, al reconocer validez y valor probatorio al

[83] CHINA: Electronic Signature Law of the People's Republic of China / Ley de la República Popular de China sobre la Firma Electrónica (2005).
Disponible en: http://www.wipo.int/wipolex/es/details.jsp?id=6559 (última visita:31/5/2014).
[84] CHINA: Certification Authority Regulations (2005).
Disponible en: http://www.novexcn.com/index.html (última visita: 31/5/2014).
[85] UN DEPARTMENT OF PUBLIC INFORMATION: Press Release. China, Singapore, Sri Lanka sign un Convention on Use of Electronic Communications in International Contracts, Nueva York, 6 de Julio de 2006.
Disponible en: http://www.un.org/News/Press/docs/2006/lt4396.doc.htm (última visita: 31/5/2014).
[86] Situación actual Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005).
Disponible en:
http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention_status.html (última visita: 31/5/2014).
[87] ARGENTINA: Ley 25.506 sobre Documento Electrónico y Firma Digital (2001).
Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm (última visita: 31/5/2014).

documento digital y autorizar el uso de la firma digital. Con esta Ley se trata de otorgar validez a la representación digital de los actos o hechos, con independencia del soporte utilizado para su instrumentación, lo que demuestra un verdadero interés de la política legislativa de avanzar en la regulación de la llamada economía digital.

1.2.6. Chile

El 12 de Abril de 2002 se publicó la Ley Nº 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firmas Electrónicas[88], de la República de Chile, que desarrolla los principio básicos, a la vez que importantes, sobre el comercio electrónico.

Esta Ley se inspira en la Ley Modelo de Comercio Electrónico principalmente, a la vez que en otras normas más recientes, como, la Directiva 1999/93/CE sobre firma electrónica; Ley Uniforme de Transacciones Electrónicas de Estados Unidos; Real Decreto Ley 14/1999, de España, sobre Firma Electrónica; el Proyecto de Ley Modelo sobre Firma Electrónica; Ley de Firmas Numéricas de Alemania; Ley de Seguridad en el Comercio Electrónico del estado de Illinois; Ley de Firma Digital del estado de California; y la Ley de Singapur sobre Comercio Electrónico.[89]

1.2.7. Reino Unido

El 25 de mayo de 2000, es aprobada la *Electronic Communications Act*[90] con el objetivo de facilitar el uso de las comunicaciones electrónicas, el almacenamiento electrónico de datos y el comercio electrónico, eliminando los obstáculos al desarrollo del comercio electrónico en el mercado interior. La Ley traspone las principales áreas abordadas en la Directiva 2000/31/CE sobre comercio electrónico: simplificar y aclarar las normas del establecimiento, garantizando la coherencia en los enfoques de las

[88] CHILE: Ley Nº 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firmas Electrónicas (2002).
Disponible: http://www.leychile.cl/Navegar?idNorma=196640 (última visita: 31/5/2014).
[89] SANDOVAL LÓPEZ, R.: "Análisis de la Ley Nº 19.799, de Firma Electrónica de la República de Chile", *Revista de la Contratación Electrónica*, núm. 32, Noviembre, 2002, pag. 23.
[90] REINO UNIDO: Electronic Communications Act (2000).
Disponible en: http://www.legislation.gov.uk/ukpga/2000/7 (última visita: 31/5/2014).

comunicaciones comerciales, asegurando la validez legal de los contratos electrónicos y la limitación de la responsabilidad de los prestadores de servicios intermediarios[91].

Asimismo, trata de poner en práctica las disposiciones de la Directiva 1999/93/CE sobre firma electrónica, a la vez que tiene en cuenta las disposiciones de la Ley Modelo de la CNUDMI sobre Firma Electrónica (2001) y la Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). A la vez que es consistente, en su alcance y propósito, con la Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005.

Esta ley se divide en tres partes[92]:

1. *Crystography Service Providers*: que venía a regular las modalidades de inscripción de los prestadores de servicios de soporte de criptografía, como los servicios de firma electrónica y servicios de confidencialidad, cuyo contenido fue derogado el 25 de mayo 2005.

2. *Facilitation of Electronic Commerce*, *Data Storage*, etc.: donde se recogen los Artículos referentes al reconocimiento legal de la firma electrónica y el proceso, en virtud del cual se pueden generar, comunicación o verificación. Además, se trata de facilitar la utilización de las comunicaciones electrónicas o de almacenamiento electrónico de información, como una alternativa a los medios tradicionales de comunicación o el almacenamiento.

3. *Miscellaneous and Supplemental*: a través de la cual se modifican los Artículos 12 y 46, b) de la Ley de Telecomunicaciones de 1984 y se inserta un nuevo Artículo 12, a) en dicha Ley. Las nuevas disposiciones se refieren a la modificación de las licencias de telecomunicaciones con excepción del cumplimiento de una referencia a la Comisión de Competencia. Esta parte también afecta a cuestiones tales como la

[91] CHISSICK, C.: *Electronic commerce: law and practice*, Londres,2001,pág.185 y ss.
[92] DEPARTMENT OF TRADE AND INDUSTRY: *Achieving best practice in your business: Information Security: Guide to the Electronic Communications Act 2000*,Londres, 2004.
Disponible en:
http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/industry_files/pdf/622.pdf (última visita: 31/5/2014).

interpretación general, el título corto, el comienzo y el alcance territorial de la presente ley.

El 8 de marzo de 2002 fue aprobada la *Electronic Signatures Regulations* 2002[93], que viene a transponer la Directiva 1999/93/CE sobre firma electrónica introduciendo los conceptos de firma electrónica avanzada y firma electrónica reconocida, así como, la supervisión y responsabilidad de los prestadores de servicios de certificación y los requisitos de protección de datos que les afectan.

1.2.8. Alemania

Alemania fue uno de los primeros Estados en dotarse de una Ley que regulara la firma electrónica[94], con el propósito de crear condiciones generales para las firmas digitales bajo las que puedan considerarse seguras y detectarse con fiabilidad las falsificaciones e imitaciones de dichas firmas digitales (Artículo 1). Así pues, trata de establecer unas condiciones básicas y generales para la implantación de una estructura segura de firmas digitales, expedición de certificados, protección de datos y regulación de componentes técnicos.

Esta Ley adoptó un enfoque prescriptivo, dando efecto legal sólo a las firmas digitales, restringiendo, el sentido de su concepto a la firma digital de claves asimétricas, certificada por un prestador de servicios de certificación, excluyéndose conceptualmente todas las demás firmas electrónicas[95]. No obstante, las demás firmas no estaban prohibidas, sino que quedaban fuera del ámbito regulatorio de la Ley, pues la Ley permitía la utilización de cualquier otro sistema de autentificación, siempre que ningún precepto legal prescribiera el uso exclusivo de la firma digital[96]. Esta Ley mostró tener, a corto plazo, falta de viabilidad práctica y fue muy criticada por poner en

[93] REINO UNIDO: The Electronic Signatures Regulations (2002).
Disponible en: http://www.legislation.gov.uk/uksi/2002/318/contents/made (última visita: 31/5/2014).
[94] ALEMANIA: Gesetz zur digitalen Signatur (Signaturgesetz - SigG) (22 de julio de 1997).
Disponible en http://www.iprecht.com/Lawyer/Contact/Download/signaturgesetz.pdf (última vista: 31/5/2014).
[95] RODRÍGUEZ ADRADOS, A.: "La firma electrónica", *Revista jurídica del Notariado*, núm. 35, 2000, págs.141-176.
[96] ADAM, J.: "Electroniche Signatur und eropäisches Privatech", *Zeitschrift für europäiches Privatech*, 2001, págs. 93 – 115.

desventaja a las empresas alemanas en las transacciones internacionales, sobre todo tras la promulgación de la Directiva sobre firma electrónica.

De esta forma, en 2001, se aprobó la Ley de condiciones marco para la firma electrónica (*Gesetz über Rahmenbedingungen für elektronische Signaturen - Signaturgesetz - SigG*)[97]. En desarrollo de esta Ley, se impulsó otra: destinada a la adopción de las formalidades de derecho privado y otras disposiciones al tráfico de los actos jurídicos modernos. Con esta Ley se procedió a la introducción de las firmas digitales en los textos básicos del ordenamiento jurídico alemán, con la pretensión de regular los contratos del siglo XXI, haciendo referencia a la posibilidad de celebrar contratos por vía electrónica, siempre que no se requiera por ley una forma específica[98].

1.2.9. Italia

La legislación italiana sobre firma electrónica comenzó a elaborarse en 1997. Así, el 15 de marzo de 1997 es aprobada la Ley italiana de 11 de marzo de 1997, número 59, sobre Delegación al Gobierno para la concesión de funciones y tareas a las regiones y a los entes locales, para la reforma de la Administración Pública y para la simplificación administrativa[99], que vino a establecer, en su Artículo 15, la validez jurídica de los documentos electrónicos elaborados tanto por entidades públicas como privadas, concretamente, su apartado segundo disponía que: "los actos, datos y documentos formados por la Administración Pública y por los particulares con instrumentos informáticos y telemáticos, los contratos estipulados en las mismas formas, así como su archivo y transmisión con instrumentos informáticos son válidos y relevantes a todos los efectos legales". Desarrollando este Artículo se aprobó, el 10 de noviembre de 1997,

[97] ALEMANIA: Gesetz über Rahmenbedingungen fürelektronische Signaturen (Signaturgesetz - SigG). (16 de Mayo de 2001).
Disponible en: http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf (última visita: 31/5/2014).
[98] FAJARDO LÓPEZ, L.: *Firma electrónica en el Derecho Privado,* Madrid, 2005, pág. 75.
[99] ITALIA: Legge n. 59/1997 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa" (17 marzo 1997).
Disponible en: http://archivio.pubblica.istruzione.it/innovazione_scuola/amministrazione/normativa/legge59_97.htm (última visita: 31/5/2014).

un Reglamento trata de aportar criterios y modalidades para la formación, el archivo y la transmisión de documentos con instrumentos informáticos y telemáticos[100].

EL 28 de diciembre de 2000 se publica el Decreto del Presidente de la República nº 445[101], texto refundido de las leyes y reglamentos relativos a los registros administrativos, que tenía por objeto regular los procedimientos con la administración electrónica en relación con los servicios públicos.

El 23 de enero de 2002 fue aprobado el Decreto Legislativo nº 10/2002[102], por el que se incorpora formalmente al ordenamiento jurídico italiano la Directiva 1999/93/CE sobre firma electrónica.

El 30 de junio de 2003 es publicado el nuevo Reglamento[103] que tiene por objetivo: a) coordinar las disposiciones del Decreto del Presidente 445/2000, sobre la firma digital y las disposiciones del Decreto Legislativo 10/2002 sobre firma electrónica; b) establecer nuevos requisitos para la realización de la actividad de certificación.

El 7 de marzo de 2005 es aprobado el Decreto Legislativo nº 82, Código de la Administración Digital[104], que viene a derogar el Decreto Legislativo 10/2002. Este Decreto Legislativo reordena y consolida la normativa vigente, propone soluciones para la actualización de la normativa italiana, a la vez que trata de corrige errores cometidos con anterioridad, respetando el sistema jurídico vigente, así como la normativa comunitaria. Esta norma tiene una gran relevancia por la especial atención que presta a las cuestiones relativas al valor jurídico y eficacia probatoria de la firma electrónica y

[100] RODRÍGUEZ ADRADOS, A.: "La firma electrónica", Revista jurídica del Notariado, núm. 35, 2000, págs.141-176.
[101] ITALIA: Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445: "Disposizioni legislative in materia di documentazione amministrativa. (Testo A)."
Disponible en: http://www.camera.it/parlam/leggi/deleghe/00443dla.htm (última visita: 2/6/2014).
[102] ITALIA: Decreto Legislativo 23 gennaio 2002, n. 10: "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche".
Disponible en: http://www.camera.it/parlam/leggi/deleghe/00443dla.htm (última visita: 6/6/2014).
[103] ITALIA: Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali".
Disponible en: http://www.camera.it/parlam/leggi/deleghe/03196dl.htm (última visita: 6/6/2014).
[104] ITALIA: Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale".
Disponible en: http://www.camera.it/parlam/leggi/deleghe/05082dl.htm (última visita: 6/6/2014).

firma digital[105]. Esta norma fue modificada por el Decreto legislativo de 4 de abril de 2006, número 159, que introdujo algunas modificaciones terminológicas, que veremos más adelante.

1.2.10. España

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica[106] es el resultado de la actualización del marco establecido en el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica[107], que tenía como objetivo fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de la empresa, los ciudadanos y las Administraciones públicas[108].

El Real Decreto-Ley 14/1999 incorporó a nuestro ordenamiento jurídico la Directiva 1999/93/CE, de 13 de Diciembre de 1999, por la que se establece un marco normativo comunitario para la firma electrónica, antes de su publicación en el Diario Oficial de las Comunidades Europeas lo que fue muy criticado[109].

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica, deroga el Real Decreto-Ley, modificando e incorporando conceptos, tales como el de firma electrónica reconocida, siguiendo las pautas establecidas por la Directiva, otorgándole equivalencia funcional con la firma manuscrita[110]; o, modificando el concepto de prestadores de servicios de certificación, concediéndole un mayor grado de libertad, reduciendo así la intervención pública[111].

---

[105] ROSELLO, C.; FINOCCHIARO, G.; TOSI, E.: *Trattato di diritto privato: diretto da Mario Bessone. Volume XXXII, Commercio Elettronico*, Torino, 2007, pág. 225.
[106] ESPAÑA: Ley 59/2003, de 19 de diciembre, de firma electrónica.
Disponible en: http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399 (última visita: 6/6/2014).
[107] ESPAÑA: REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.
Disponible en: http://www.boe.es/buscar/doc.php?id=BOE-A-1999-18915 (última visita: 6/6/2014).
[108] ILLESCAS ORTIZ, R.: "La firma electrónica y el R.D. Ley 14/1999, de 17 de septiembre", *Derecho de los negocios*, núm. 109, octubre 1999, págs.1-14.
[109] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, págs.30 y ss.
[110] ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica,* Madrid, 2009, pág.143 y ss.
[111] MARTINEZ NADAL, A.: *Cometarios a la ley 59/2003 de Firma Electrónica*, Madrid, 2009, pág. 316 y ss.

En definitiva, la Ley de firma electrónica se inspira en la Directiva, que a su vez se inspira en la Ley Modelo sobre Firma Electrónica. De esta forma, es consciente de que la firma electrónica es un elemento esencial del comercio electrónico: da respuesta a la necesidad de conferir seguridad a las comunicaciones y transacciones, siendo por ello vital el vínculo entre la fiabilidad técnica y la eficacia jurídica que cabe esperar de la firma electrónica[112].

Se pretende potenciar el mercado on-line, ofreciendo, ante todo, seguridad en las transacciones, afianzándose la firma electrónica como el instrumento adecuado capaz de devolver la credibilidad y confianza a los sujetos intervinientes a través de sus propios ordenadores, ya sea a nivel nacional o internacional. Mediante esta Ley, España crea un entorno jurídico para todo medio técnico viable de comunicación comercial, a través del empleo de los medios electrónicos enunciados en ella a nivel nacional. Sin embargo, desde una perspectiva internacional, la firma electrónica y el medio electrónico en el que se desenvuelve implica un reconocimiento de la misma, clave y con gran transcendencia jurídica, importancia que se aprecia a la vista de las diferentes regulaciones estatales estudiadas, a fin de garantizar su validez jurídica.

En la actualidad, se está trabajando en un nuevo Código Mercantil[113], inspirándose en las Leyes Modelo de CNUDMI/UNCITRAL sobre contratación y firmas electrónicas de 1.996 y 2001 respectivamente, con el fin de regular las formas especiales de celebración de contratos mercantiles que las nuevas tecnologías y la práctica han consagrado, poniendo en práctica los grandes principios de la contratación electrónica, esto es, la equivalencia funcional, la neutralidad tecnológica, la inalteración del derecho preexistente, la libertad de pacto y la buena fe.

El nuevo Código, de momento se abstiene de legislar sobre la firma electrónica por entender que su uso y disciplina, si bien han surgido en el ámbito negocial y mercantil, se encuentran en la actualidad extendidas a la gran mayoría de las actividades

[112] MADRID PARRA, A.: "Seguridad en el comercio electrónico" en *Contratación y comercio electrónico*, (Orduña Moreno, F. (Dir.), Campuzano Laguillo, A.B.; Plaza Penadés, J. (Coords.)), Valencia, 2003, pág. 130.

[113] El 30 de mayo de 2014 fue presentado el Anteproyecto de Ley de Código Mercantil. Actualmente se encuentra en tramitación, en fase de información al Consejo de Ministros.
Disponible en: http://www.mjusticia.gob.es/cs/Satellite/es/1215198252237/ALegislativa_P/1288774452773/Detalle.html (última visita: 24/10/2014).

documentales y a las diferentes ramas del ordenamiento. Sin embargo, cuestiones de importancia práctica, carentes hasta el momento de disciplina[114] de rango superior, adquieren estatuto legal en esta ocasión; tal es el caso de la factura electrónica, la solución de los problemas derivados del intercambio de soportes documentales o la cada vez más utilizada y en más elevadas cuantías contratación electrónica automatizada[115].

1.3. Plano extraestatal

Dentro del panorama de las instituciones electrónicas existen organizaciones de ámbito internacional que han tratado cuestiones relativas al comercio electrónico y a la firma electrónica, a través de documentos que muestran un gran interés por la armonización del mercado electrónico internacional.

Estas organizaciones tienen una gran actividad, a la vez que muestran su gran influencia respecto a los propios Estados y otras organizaciones internacionales, pues es frecuente que acudan a las reuniones de la CNUDMI e incluso elaboren documentos sobre cuestiones a debatir en las reuniones de ésta. De esta forma, la CNUDMI mantiene estrechos vínculos con organizaciones de ámbito internacional y regional, tanto intergubernamentales como no gubernamentales, que participan activamente en el programa de trabajo de la CNUDMI y se ocupan en general de cuestiones de derecho mercantil internacional, para facilitar el intercambio de ideas y de información[116].

[114] Este Proyecto de Ley de Código Mercantil se encuentra en total sintonía con los trabajos que se están desarrollando en la CNUDMI sobre documentos electrónicos transferibles. Véase, en el apartado de este mismo capítulo referente a la actividad de la propia CNUDMI posterior a la Convención de 2005.

[115] Así, el Artículo 421,7 de la Propuesta de Código Mercantil elaborada por la Sección de Derecho Mercantil de la Comisión General de Codificación, intitulado "Documento y firma electrónicos" dice: "1. Toda comunicación electrónica goza de la naturaleza de documento electrónico de acuerdo con las disposiciones aplicables de la legislación sobre firma electrónica. 2. Toda comunicación electrónica emitida con fines negociales habrá de poder ser atribuida a su emisor. A tal fin, salvo disposición o pacto en contrario, podrá ser utilizada una firma electrónica apropiada a los fines perseguidos y las circunstancias del caso".

[116] Organizaciones con quien colabora la CNUDMI.
Disponible en: http://www.uncitral.org/uncitral/es/tac/coordination.html (última visita: 31/5/2014).

1.3.1. Cámara de Comercio Internacional (CCI)

La Cámara de Comercio Internacional[117] es una institución de gran importancia en el ámbito mercantil. En 1995, a raíz de un estudio sobre los aspectos jurídicos del comercio electrónico, comenzó a trabajar en el desarrollo de unas directrices de carácter internacional para promover el comercio electrónico y el empleo de medios electrónicos en las transacciones internacionales[118]. En 1997 elaboró una recopilación de principios relativos a las firmas electrónicas conocida como la GUIDEC, cuyo objeto era favorecer la capacidad de la comunidad internacional para concluir transacciones electrónicas seguras a través de internet, para ellos incluye una terminología uniforme y un conjunto de buenas prácticas[119].

La GUIDEC fue actualizada en 2001, aprobándose la GUIDEC II, que profundizó, desarrolló y actualizó aspectos de la primera, partiendo de las bases ya establecidas, con respecto a la autenticación de las firmas electrónicas digitales, trata de proponer una autoridad reconocida en relación con el prestador de servicios de certificación.

En 2004, elaboró unas cláusulas contractuales para su utilización en el comercio electrónico y tienen por objeto dotar de mayor certeza o seguridad jurídica a todo contrato que se vaya a concertar por vía electrónica; trata de dos breves cláusulas fáciles de incorporar a su contrato, estipuladas en términos claros, de tal manera que las partes puedan quedar obligadas por los términos del contrato concertado por vía electrónica, ya sea a través de Internet, por correo electrónico o por EDI. Estas cláusulas no afectan, en modo alguno, al contenido del contrato, ni interfieren con ninguna de sus condiciones; simplemente facilitan la negociación por vía electrónica de un contrato[120].

---

[117] CAMARA DE COMERCIO INTERNACIONAL.
Disponible en: http://www.iccwbo.org/ (última visita: 31/5/2014).

[118] PEREZ PEREIRA, Mª.: Firmas Electrónicas: Contratos y Responsabilidad Civil, Navarra, 2009, pág.92.

[119] DE MIGUEL ASENSIO, P. A.: *Derecho privado de Internet*, Madrid, 2011, pág.905.

[120] CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.113 - Aspectos jurídicos del comercio electrónico: Cláusulas contractuales 2004 de la CCI para el comercio electrónico (ICC eTerms 2004). Guía de la CCI para la contratación electrónica*, Viena, 11 a 22 de octubre de 2004.

1.3.2. American Bar Association (ABA)

La *Amercican Bar Association* (ABA)[121] ha desempeñado un papel muy importante en materia de comercio electrónico y firma electrónica, hasta tal punto que sus textos han sido muy tenidos en cuenta por UNCITRAL, la Cámara de Comercio Internacional e incluso ha influenciado en la regulación normativa de Estados Unidos y la Unión Europea.

Su actividad, en esta materia, comenzó en 1989 con la publicación del *Model Trading Partner Agreement*, realizado por el *Electronic Messaanging Services Task Force* y el *Subcommitte on the Uniform Commercial Code* de la ABA, se trata de un modelo de acuerdo EDI concebido para las relaciones de ámbito nacional en los Estados Unidos[122].

Posteriormente publicó otro texto de gran importancia la *Digital Signature Guidelines* en 1996[123], con la finalidad de ayudar a esclarecer la interpretación de la legislación sobre firmas electrónicas digitales y las autoridades de certificación, así como ayudar en su legislación. Estas Directrices fueron actualizadas en 2003 a través de *PKI Assessment Guidelines*[124] intentando proporcionar una herramienta mediante la cual las personas puedan evaluar la tecnología PKI y su confiabilidad, explicar los modelos básicos de evaluación de la PKI, terminología evaluación PKI y consecuencias, proporcionar una guía para la selección de las políticas, normas y acuerdos legales, incluyendo políticas de certificación, las declaraciones de prácticas de certificación,

[121] AMERICAN BAR ASSOCIATION.
Disponible en: http://www.americanbar.org/aba.html (Última visita:31/5/2014).

[122] CRUZ RIVERO, D.: "Análisis del concepto de firma electrónica como equivalente de la firma manuscrita", Revista de la Contratación Electrónica, núm. 60, mayo, 2005, pág. 3 – 122.

[123] SECURITY COMMITTEE ELECTRONIC COMMERCE AND INFORMATION TECHNOLOGY DIVISION SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION: *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, agosto, 1996.
Disponible en:
http://www.americanbar.org/content/dam/aba/events/science_technology/2013/dsg_tutorial.authcheckdam.pdf (última visita: 31/5/2014).

[124] SECURITY COMMITTEE ELECTRONIC COMMERCE AND INFORMATION TECHNOLOGY DIVISION SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION: *PKI Assessment Guidelines: guidelines to help assess and facilitate interoperable trustworthy public key infrastructures*, mayo, 2003.
Disponible en:
http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf (última visita: 31/5/2014).

promover la interoperabilidad fluida entre diferentes PKI y sus componentes, así como proporcionar un marco para la comprensión de los servicios de PKI, productos, tecnologías y conceptos jurídicos emergentes.

Más recientemente, en 2012, el equipo de tareas *Identity Management Legal Task Force* de la *American Bar Association* presentó a la Secretaría de la CNUDMI un documento sobre el panorama general de la gestión de la identidad digital, ofreciendo una visión acerca de la gestión de la identidad digital, su función en el comercio electrónico, las cuestiones jurídicas que plantea y las barreras legales que plantea. Este documento se centra en los sistemas de gestión de las identidades comerciales concebidas para su utilización en el contexto empresarial, en particular en las comunicaciones entre empresas, entre empresas y gobiernos y entre empresas y consumidores[125].

1.3.3. Aplicaciones prácticas al mercado: creciente consenso internacional

1.3.3.1. Protcolos SET y SSL

1.3.3.1.1. Introducción

Hay varios enfoques para proporcionar seguridad en la web, concretamente en los medios de pago. En todo pago que se realiza por Internet se corren riesgos. Estos riesgos vienen desde la suplantación de la identidad del comprador, a la suplantación del vendedor, de intrusismos en la propia comunicación, hasta el propio almacenamiento de datos en servidores no seguros.

De estos riesgos ha nacido la necesidad de establecer métodos de pago que puedan dar autenticación, confidencialidad, no repudio e integridad a las transacciones

[125] CNUDMI/UNCITRAL: A/CN.9/WG.IV/WP.120 - Panorama general de la gestión de la identidad digital. Documento de *antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre a 2 de noviembre de 2012.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última vistas: 31/5/2014).

comerciales que pretendan realizar las partes de tal manera que se reduzca al mínimo los riesgos mencionados.

En los parámetros que nos movemos, resulta esencial probar la identidad de los agentes que participan en la transacción económica, pues, el comerciante o el banco necesitan saber la identidad del comprador para evitar el repudio y el comprador debe estar seguro de que dialoga con quien cree que debe hacerlo para que todo salga bien.

De esta manera, los comerciantes que aceptan pagos por Internet utilizan servidores web; esta web proporciona la posibilidad de introducir los datos del medio con el que se pagara la compra; ante esto, se deben tener en cuenta los mecanismos de seguridad y la situación por la que surgieron los protocolos SSL y SET.

1.3.3.1.2. Protocolo SSL

El protocolo SSL (*Secure Soket Layer*) fue desarrollado por la compañía Netscape en 1994. Se trata de un protocolo de propósito genérico que permite el establecimiento de conexiones seguras. Proporciona servicios de seguridad, cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.

Aunque en principio no se diseñó específicamente para las aplicaciones de comercio electrónico; sin embargo, es el más utilizado actualmente en los pagos que se realizan en la web. Está implementado, por defecto, en los navegadores y servidores web más populares, lo que facilita su uso. No obstante, el que no se pensase para pagos electrónicos hace que no se garantice ciertos requisitos que deberían darse en este tipo de transacciones[126].

Al hablar de SSL[127] debemos tener presentes dos conceptos:

[126] PÉREZ GIL, J.: "La prueba del pago por medios electrónicos", en *Los medios electrónicos de pago: problemas jurídicos* (Dir. Mata y Martín, R. M. Coord. Javato Martín, A. Mª), Madrid, 2007, pags.19 y ss.

[127] DORAL, A.: *Seguridad en internet y medios de pago*, Madrid, 2002, pág. 47.

a) Conexión: una conexión es un transporte que proporciona un tipo de servicio idóneo Para SSL, tales conexiones son relacionadas de igual a igual. Las conexiones son transitorias y cada conexión está asociada con una sesión.

b) Sesión: una sesión SSL es una asociación entre un cliente y un servidor. Las sesiones definen un conjunto de parámetros criptográficos de seguridad, que pueden compartir entre múltiples conexiones. Las sesiones se usan para evitar el costoso proceso de negociación de nuevos parámetros de seguridad para cada conexión.

SSL proporciona seguridad mediante el cifrado del canal de comunicación establecido entre el consumidor y el comercio. El certificado del servidor permite garantizar la autenticidad del servidor frente a los posibles compradores (mediante certificados digitales X.509) y la confidencialidad e integridad (mediante encriptación); es decir, cuando un usuario se conecta con un navegador o con un servidor SSL puede saber que está en conexión segura porque la URL comienza por "https" en vez de "http", además de un candado cerrado indicándose así que estamos en una conexión segura.

El protocolo SSL está basado fundamentalmente en el algoritmo RSA[128], es decir, cuando un usuario desea iniciar una comunicación segura, por ejemplo, para realizar una compra on-line y comunicar los datos de su tarjeta de crédito, su servidor abre un canal codificado con el servidor de destino, con quien negocia una serie de mejoras en la seguridad de la comunicación (pasándose de "http" a "https")[129].

Sin embargo, el comercio no puede realizar la identificación de la persona que quiere realizar la compra salvo que éste sea titular de un certificado. Por otra parte, el pago no se realiza de una forma automática, sino que el titular tiene que introducir todos los datos personales y de tarjeta de crédito en una plantilla y enviarla a través de la comunicación segura establecida mediante SSL. Este proceso deberá repetirse cada vez que se quiera realizar una compra a no ser que el web disponga de alguna tecnología

[128] DORAL, A.: *Seguridad en internet y medios de pago*, Madrid, 2002, pág. 45.
[129] DORAL, A.: *Seguridad en internet y medios de pago*, Madrid, 2002, pág. 47.

tipo "carro de compra". Para verificar si un comercio está utilizando SSL basta con comprobar la URL del comercio y ver que en vez de "http" aparece "https".

Por ello, este sistema plantea dos inconvenientes, fundamentalmente:

a) Sólo pueden realizarse transacciones punto a punto: SSL únicamente maneja interacciones punto a punto; es decir, solo asegura la interacción entre dos interlocutores, normalmente comprador y vendedor. Mientras que las transacciones con SET, diseñado para pagos con tarjetas de crédito, involucran como mínimo a tres partes: el titular, el comerciante y el banco emisor de la tarjeta.

b) Con SSL los datos de la tarjeta de crédito del cliente se mantienen en el servidor del comercio por lo que son vulnerables a un ataque externo. Por otra parte, los comerciantes no tienen asegurada la veracidad de los datos de la tarjeta enviados por el cliente.

SSL no es un protocolo diseñado para pagos electrónicos, sino para garantizar la seguridad en la comunicación entre servidores web. Por lo tanto, aunque garantiza la seguridad en la comunicación y la autenticación del servidor, no garantiza la autenticación del cliente ni ofrece mecanismos para evitar el repudio. Esto ha facilitado el fraude especialmente en los sitios web donde se descargan contenidos, ya que el estafador tiene garantizado el anonimato[130]. Otro riesgo que la utilización de SSL tampoco evita es el que se supone para el comprador dar sus datos bancarios al comerciante, lo que abre la puerta del fraude.

1.3.3.1.3. Protocolo SET

En 1997 varias empresas de tarjetas de crédito (VISA Internacional y MasterCard Internacional) decidieron elaborar un método seguro para el comercio electrónico por

[130] PÉREZ GIL, J.: "La prueba del pago por medios electrónicos", en *Los medios electrónicos de pago: problemas jurídicos* (dir. Mata y Martín, R. M. Coord. Javato Martín, A. Mª), Madrid, 2007, pags. 19 y ss.

Internet, fijando tres objetivos comerciales: la solución tenía que ser segura y abierta a cualquier proveedor de tecnología interesado en elaborar un producto que cumpliera el protocolo definido y todas las aplicaciones debían ser practicables entre sí.

Al hablar de tarjetas de pagos por Internet, el término seguro pasa a ser un término esencial por: el carácter reservado de los datos (número de cuenta), la integridad de la información sobre los pedidos y la autenticación de las partes en la operación. Estas especificaciones suponen la adopción de nuevos procedimientos en relación con los actuales procesos utilizados en la actualidad, debiendo crearse nuevos mecanismos de seguridad, nuevos métodos de autenticación de la titularidad de la tarjeta a la vez que surge la necesidad de crear mecanismos que permitan al titular asegurarse de que la transacción comercial que pretende realizar acepta ese medio de pago.

En este contexto nace el protocolo SET (*Secure Electronic Transaction*) con el fin de garantizar la seguridad en las compras por tarjetas de crédito realizadas a través de Internet, y, de esta manera, motivar la aceptación del comercio electrónico y evitar el desarrollo de soluciones propietarias que no pudieran interoperar para garantizar una funcionalidad universal.

Hablar de protocolo SET es hablar de otro intento más en alcanzar la seguridad en las transacciones electrónicas. Y se hace a través del uso de firmas numéricas (basadas en el modelo X.509) para cumplir la función de integridad de los datos y autenticación de las partes.

1.3.3.1.3.1. Firmas numéricas

Se basa en la criptografía de clave pública. Los certificados numéricos son documentos electrónicos firmados numéricamente por una entidad de confianza[131]. Cuando un documento está numéricamente firmado, se le adjunta una copia del certificado numérico del signatario, que contiene información sobre la persona y sobre

[131] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE (2001)*, párr. 33.

su clave pública. Al recibir el mensaje y el certificado numérico, el receptor utiliza la clave pública en el certificado numérico para autenticar el mensaje.

Los certificados numéricos utilizan la norma ISO X.509 que permite una jerarquía de entidades de confianza utilizadas para autenticar a las partes. Este método se denomina de la tarjeta de crédito, por el hecho de que refleja el modelo comercial de la tarjeta de crédito.

La firma digital de un documento conforme al método X.509 implica el envío del certificado digital al signatario y de todos los certificados digitales auxiliares relacionados con la jerarquía de entidades de confianza. Según ese modelo, el receptor puede verificar toda la cadena de entidades de confianza sin tener que consultar la guía en línea. Una de las ventajas de este método es la posibilidad de relacionar muchos certificados con una raíz de confianza, que constituye también un punto débil. Por consiguiente, si esa raíz está en algún momento en entredicho, todo lo que pude venir después perderá credibilidad[132].

1.3.3.1.3.2. Características

Como hemos dicho, SET se centra en el empleo de tarjetas de pago en la compra electrónica pretendiendo instaurar una forma extendida de pago a través de internet con el mismo nivel de garantía y seguridad que el mundo físico.

Su funcionamiento podría resumirse en lo siguiente[133]: el consumidor desea comprar a través de Internet, y especifica los bienes y servicios que desea adquirir, seleccionando el medio de pago e iniciando la operación. La información de pago llega firmada numéricamente a la institución financiera. Por otro lado, la información del pedido por y la información de pago parte del consumidor llega al comerciante firmada numéricamente también. Cuando el comerciante recibe el mensaje de pedido se separa la información de pago formulada en clave, firma numéricamente este nuevo mensaje y lo envía a la institución financiera. La institución financiera verificaría la firma digital

[132] CNUDMI/UNCITRAL: *Anuario: volumen XXIX: 1998*, Nueva York, 2001, párr. 97 y ss.
[133] Funcionamiento SET.
Disponible en: www.setco.org (última visita: 6/6/2014).

del comerciante, descifraría la información de pago y procesaría esa información a través de la infraestructura existente de pagos. La institución financiera firma numéricamente la respuesta de autorización y la envía al comerciante que, a su vez, envía una respuesta firmada numéricamente. Si la operación es autorizada, el comerciante ha de cumplir con el pedido.

Es decir, SET lo que propone es firmar digitalmente los mensajes de una operación con una única firma, creando una firma dual. De tal manera que la firma se emplea para vincular un mensaje de orden de pedido enviado al comercio, con órdenes de pago que contiene información de una cuenta, enviada por el adquirente. Cuando el comercio envía una petición de autorización al adquirente, incluye órdenes de pago enviadas por el titular y el resumen de la orden de pedido. El adquirente emplea el resumen del mensaje del comercio y calcula la sintesis del mensaje de las órdenes de pago para comprobar la firma dual.

De esta forma, se observa la dependencia respecto de la tecnología de las firmas numéricas en la autenticación de mensajes y de partes. No obstante, los certificados SET no son certificados de identidad de nadie ni pueden utilizarse con este fin. Los certificados SET se limitan a autenticar la relación de una clave pública con un número de cuenta.

Así, podemos afirmar que:

a) Se utilizan firmas numéricas y certificados sin fines de identidad.

b) Se produce una emisión de certificados por entidades certificadoras sin licencia y basadas en el mercado.

c) La emisión de certificados en un sistema en que las partes han definido sus derechos y obligaciones.

d) En algunos casos, una parte en la que se confía (el banco que realiza el pago sobre la base de la información firmada numéricamente por el consumidor) podía ser el emisor del certificado.

1.3.3.1.3.3. Interoperabilidad

La interoperabilidad es un elemento esencial de SET. Esto supone que, cualquier titular de una tarjeta, debe poder comunicarse con cualquier comercio que se encuentre acogido al protocolo SET. Como sabemos, con la interoperabilidad conseguimos la seguridad del buen fin de la operación. Esto convierte a SET en un protocolo abierto, no porque cualquiera pueda decidir utilizarlo al navegar por Internet, sino porque se consigue superar toda posibilidad de entrar en competición entre los diferentes sistemas desarrollados[134].

1.3.3.1.4. SET vs SSL

Como hemos visto, SET se caracteriza por cubrir de forma segura solo el proceso del pago, no de toda la transacción, quedando fuera de su ámbito de actuación las fases de negociación y entrega y, además, identifica a todas las partes en virtud de la firma dual que utiliza. SSL sirve para proteger la información en tránsito y, además, da autenticidad del servidor al cliente, aunque es cierto que los servicios de seguridad son limitados, pues no proporciona no repudio en origen.

De este modo, podemos pensar que ambos protocolos no compiten entre sí, sino que más bien han de complementarse, utilizándose en SSL en las fases previas y posteriores a la fase de pago y SET para esta fase concreta[135]. Así, vemos como SSL no es la vía más adecuada para realizar pagos con tarjetas de crédito a través de Internet, siendo recomendable SET. No obstante, hemos de hacer una apreciación, SET corrige las deficiencias de SSL pero es menos utilizado.

[134] BRAYGUAL, F. A.: "Capítulo IX: Protocolo SET" en *Régimen jurídico de internet* (coord. Cremades, J.; Fernández-Ordóñez, M. A; Illescas, R), Madrid, 2002, pág. 345.
[135] CNUDMI/UNCITRAL: *Anuario: volumen XXIX: 1998*, Nueva York, 2001, párr. 97 y ss.

1.3.3.2. Identrus

En fecha de 6 de Abril de 1999, Identrus[136] es creada por las mayores instituciones financieras del mundo, mediante la fundación de una empresa de responsabilidad limitada (acuerdo ERL), sometida a la legislación del Estado de Delaware (Estados Unidos). Identrus se sustenta sobre dos pilares legales: el primero es la *Electronic Signature in Global and Nacional Commerce Act* de Estados Unidos; y, el segundo, el régimen fiscal y mercantil del Estado de Delaware. Su objeto social es gestionar red mundial e interoperativa entre entidades financieras que ofrezcan servicios de autoridad certificante y poner la infraestructura necesaria para ello[137].

Identrus surge en un contexto marcado por: la falta del reconocimiento legal de la firma electrónica para las transacciones rápidas y seguras, la inexistencia de autoridades de certificación mundiales que expidan certificados intercambiables a nivel internacional, la variedad de sistemas informáticos utilizados y los grandes obstáculos generales en las relaciones interempresariales.

De esta manera, a medida que el volumen y la importancia del comercio electrónico aumentan, se hace necesario añadir políticas de autentificación de identidad y procedimientos para dar confianza al mercado a través de medios electrónicos seguros y legalmente vinculantes. Identrus ayuda a definir e implementar las estrategias de identidad, protección de sus clientes y reducción de los riesgos de actividad fraudulenta. Para ello, es capaz de proporcionar servicios de consultaría para ayudar a cumplir dichas estrategias[138.]

---

[136] IDENTRUS.
Disponible en: http://www.identrust.com/index.html (última visita: 6/6/2014).

[137] MLA BUSINESS/TECHNOLOGY EDITORS: *Identrus, LLC to Acquire Digital Signature Trust; Merger Aligns U.S. Financial Services Community and TrustID with the Identrus Global Standard for Identity Authentication*, 2002.
Disponible en: http://presseservice.pressrelations.de/standard/result_main.cfm?aktion=jour_pm&r=90892&quelle=0&pfach=1&n_firmanr_=100687&sektor=pm&detail=1 (última visita: 6/6/2014).

[138] IDENTRUS:
Disponible en: www.identrust.com (última visita: 6/6/2014)

Hoy día, Identrus ofrece sus servicios a Bancos (proporcionando un estándar de identidad común y una plataforma interoperable a través de geografías, empresas y aplicaciones)[139], a empresas (protegiéndoles de un posible fraude en línea, y les ayuda en los procesos de simplificación a la hora de autenticar, cifrar y crear la firma electrónica, en todas las partes del mundo para cada tipo de transacción o actividad. Además, puede utilizar la firma electrónica para firmar un contrato o acceder a sus cuentas bancarias o autorizar un pago)[140] y a Gobiernos[141].

Identrus ofrece un conjunto de reglas de confianza para la autentificación de la identidad que fue creado por las instituciones financieras mundiales. Estas reglas las llama P.L.O.T.: Política, marco legal, operaciones de alojamiento y tecnología[142]. Este conjunto de reglas aseguran que las identidades se emitan y se utilicen de forma estandarizada dentro y fuera de una institución financiera, nacional o internacional. Como resultado de ello las identidades Identrus son interoperables a nivel mundial.

Por otro lado, en abril de 1999, la Comisión recibe la notificación de un conjunto de acuerdos relativos a la creación de una red de instituciones financieras que actuarán como autoridades de certificación de operadores fiables de comercio electrónico, en principio únicamente de empresa a empresa[143].

Las partes[144] han formado una empresa en participación, Identrus, LLC, sociedad de responsabilidad limitada constituida con arreglo a la legislación de Estados Unidos de América. Identrus aportará y gestionará la infraestructura necesaria para crear una red global e interoperable entre instituciones financieras que ofrecen servicios de autoridad de certificación ("sistema identrus").

---

[139] IDENTRUS:
Disponible en: www.identrust.com/banks/index.html (última visita: 6/6/2014)
[140] IDENTRUS:
Disponible en: www.identrust.com/corporates/index.html (última visita: 6/6/2014)
[141] IDENTRUS:
Disponible en: www.identrust.com/goverment/index.html (última visita: 6/6/2014)
[142] SOLUCIONES INDENTRUS (PLOT: Policies, Legal Framework, Operations Hosting and technology):
Disponbile en: Www. Identrust.com/solutions/plot.html. (última visita: 6/6/2014)
[143] COMISIÓN EUROPEA: *Comunicación de la Comisión a tenor del apartado 3 del artículo 19 del Reglamento nº 17 del Consejo relativa al asunto COMP/27.462 – Identrus (2000/C 231/03)*, DOUE, núm.3, 11 de agosto 2000.
[144] ABN AMRO Service Company, Inc.; BA Interactive Service Holding Company, Inc.; Barclays Electronic Commerce Holding Inc.; Bayerische Hypo- und Vereinsbank AG.; The Chase manhattan Bank; Citibank NA.; Deutche Bank AG.; Pyramid Ventures Inc.

Identrus estará participada por un número limitado de entidades, pero ninguna en solitario tendrá control sobre Identrus. La participación estará abierta a instituciones financieras cualificadas de todo el mundo ("participantes"), que competirán entre sí en los mercados de referencia.

La Comunicación de la Comisión, nos desglosa la sociedad, su participación en el sistema, la forma de adopción de acuerdo y los mercados de referencia a nivel geográfico y de productos. Identrus presenta un objetivo claro: promocionar operaciones y gestión de infraestructuras para hacer seguras las transacciones de comercio electrónico; observando que cumple con todos los principios básicos de la Ley Modelo de la CNUDMI sobre Firma Electrónica[145]:

- Neutralidad tecnológica (Identrus aporta la infraestructura, es decir, se ocupa del diseño y operación de la infraestructura, que permitirá a las instituciones financieras participar en el sistema y convertirse en autoridades de certificación gestionando los riesgos inherentes).

- No discriminación (el éxito del sistema de certificación se basa en su interoperabilidad con otros sistemas. El único requisito para que puedan convertirse en participes de Identrus son requisitos de capital, definidos por el Comité de Basilea de supervisión bancaria y ciertos requisitos de fiabilidad).

- Autonomía de las partes (Identrus es una autoridad de certificación básica respecto de las autoridades de certificación participantes. No ofrece servicios a los usuarios finales directamente. Son los participantes los que prestan los servicios a las empresas ejerciendo su papel de autoridad certificadora).

- Su internacionalidad queda puesta de manifiesto con la prestación de sus servicios a nivel mundial.

[145] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE (2001)*, Nueva York, 2002, párr.4 y ss.

El 31 de Julio de 2001, la Comisión se pronuncia mediante la Decisión de la Comisión de 31 de Julio de 2001146. Esta Decisión tiene en cuenta el marco legislativo existente[147]; la falta de un medio extensivo, seguro y eficaz de hacer pagos transfronterizos[148]; y la falta de existencia de servicios mundiales de autoridades de certificación en redes abiertas, y, así, se reconoce que los riesgos, no nuevos, pero si de importancia creciente, asociados a la prestación en línea de servicios financieros y de autentificación podrían desembocar en importantes riesgos legales y de reputación[149].

De esta manera, analiza observaciones presentadas por terceros en contra de la apertura del sistema de certificación Identrus, que mostraban su inquietud por temor a la creación de un "cartel tecnológico" que rompiera el equilibrio competitivo[150]. La Comisión se pronuncia con respecto a la creación del sistema Identrus diciendo que no implica cierre del mercado, pues: opera en un mercado nuevo en pleno desarrollo; existe competitividad ABAecom, SWIFT, VISA y Mastercard, por ejemplo; y, por último, los participantes son libres de participar en otros sistemas similares.

1.3.3.3. Sistema bolero

1.3.3.3.1. Introducción

En los años 80, fueron muchos los intentos llevados a cabo a fin de crear documentos electrónicos de transporte, algunos de iniciativa privada (de la banca principalmente) y otros fruto de la labor de organizaciones internacionales como el Comité Marítimo Internacional (CMI), UNCITRAL o la CCI, aunque no tuvieron mucho éxito.

---

[146] COMISIÓN EUROPEA: Decisión de la Comisión de 31 de Julio de 2001 relativa a un procedimiento con arreglo al Artículo del Tratado 81 del Tratado CE y el Artículo 53 del Acuerdo EEE. (Asunto COMP/37.462 – Identrus). Notificada con el número C (2001) 1850. (2001/696/CE).
Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32001D0696 (última visita: 6/6/2014).
[147] Considerando 6 de la Decisión de la Comisión de 31 de Julio de 2001.
[148] Considerando 7 de la Decisión de la Comisión de 31 de Julio de 2001
[149] Considerando 8 de la Decisión de la Comisión de 31 de Julio de 2001.
[150] Considerando 39 de la Decisión de la Comisión de 31 de Julio de 2001.

En abril de 1994, comenzó a elaborarse el sistema BOLERO fue llevado a cabo con el fin de fomentar el uso de conocimientos de embarque electrónico. Nació por iniciativa de la Comisión Europea[151], formando parte del referido proyecto además empresarios de transporte, bancos, importadores, exportadores y compañías de telecomunicaciones.

En 1997, tras la incorporación de la *Society for Worldwide Interbank Financial Transactions* (SWIFT) y la *Throught Transport Mutual Inssurance Association Ldt* (TTC) el proyecto comenzó a tener éxito. En 1998 se constituyó *Bolero Operations Ldt* bajo la administración de SWIFT y TTC. El sistema fue puesto en servicio finalmente en 1999 obteniendo una gran acogida por los protagonistas del tráfico jurídico.

Bajo el nombre de BOLERO podemos distinguir dos personas jurídicas, la *Bolero Association Limited* y la *Bolero Internacional Limited*. La primera es una persona jurídica que representa a los usuarios del sistema BOLERO, además de celebrar contratos de prestación de servicios BOLERO. La segunda, con sede en Londres, surge a iniciativa privada en 1995, por un grupo de empresas con la intención de crear una plataforma de comercio electrónico internacional; formándose una sociedad que ha desarrollado el sistema BOLERO, respondiendo a las inquietudes e intereses privados, para lo que crea una infraestructura tecnológica y jurídica que aporta al tráfico económico una mayor agilidad, incluyendo técnicas que eliminan los problemas transfronterizos existentes.

Su objetivo[152] no es otro que el de promover estándares internacionales para el comercio electrónico, así, como, actuar como un foro de empresas para aspectos relacionados con las prácticas comerciales electrónicas en el comercio internacional, promoviendo un marco jurídico seguro para los documentos de transporte marítimo, etc.[153].

[151] Fue financiado en parte por la UE en el contexto del Programa Infosec (DGXIII) y en parte por empresas comerciales interesadas.
[152]BOLERO.
Disponible en: www.boleroassociation.org (última visita: 5/6/2014).
[153] BOLERO: marco jurídico.
Disponible en: http://www.bolero.net/en/home.aspx (última visita: 5/6/2014).

1.3.3.3.2. Características y funcionamiento

Las principales características que definen el funcionamiento del sistema BOLERO son su carácter contractual y cerrado. Asimismo, es un sistema integrador diseñado para comunicar y gestionar no sólo conocimientos de embarque, sino casi cualquier documento relacionado con el comercio internacional (hasta 60 tipos de documentos), como órdenes de compra, waybills, certificados de origen, certificados de seguro, instrucciones de embarque y licencias de exportación[154]. Los usuarios del sistema realizan sus operaciones en el interior de un único marco contractual que se recoge en el reglamento de la BOLERO Association Ldt cuya aplicación resulta obligatoria para estos.

Las partes que pretendan integrarse en el mencionado sistema deben adherirse a su Reglamento (*Rulebook*)[155] que ofrece las ventajas inherentes a la transmisión electrónica de datos; esto es, la reducción de los ciclos temporales en que se desarrollan las operaciones y de los costes de las transacciones, todo ello unido a un elevado nivel de seguridad en las comunicaciones, lo que implica garantías en cuanto a su autenticidad, integridad, confidencialidad y perdurabilidad, que se consigue gracias al sistema de certificaciones o de firma digital[156]**.** Las *Rulebook* aparecen agrupadas en tres bloques y un anexo. La primera parte está destinada a definiciones; la segunda se contienen previsiones de carácter general, tales como el ámbito de aplicación, las normas relativas a las seguridad de los mensajes, las consecuencias de la renuncia a la utilización del sistema BOLERO; y, finalmente, la tercera establece el régimen al que queda sometido el *Bolero Bill of Landing*.

A través de las *Rulebook*, los usuarios se comprometen a reconocer la validez y eficacia a la comunicación electrónica mantenida entre ellos así como a aceptar que los mensajes firmados digitalmente les vinculan y, de otra, este reglamento se rige e interpreta de acuerdo con la Ley inglesa.

---

[154] GUERRERO LEBRÓN, Mª J.: "El crédito documentario electrónico y su nueva regulación", *Revista de la Contratación Electrónica*, Núm. 34, 2002, p. 3 – 64.
[155] Disponible en: http://www.bolero.net/en/Newsdownloads/articlesordownloads.aspx (última visita: 15/3/2014).
[156] GUERRERO LEBRÓN, Mª J.: "El crédito documentario electrónico y su nueva regulación", *Revista de la Contratación Electrónica*, Núm. 34, 2002, p. 3 – 64.

El funcionamiento del sistema BOLERO podría resumirse del siguiente modo: el cargador interesado en la celebración de un contrato de transporte envía un mensaje electrónico al porteador que contiene los datos descriptivos de la mercancía objeto del transporte. El porteador tras aceptar la oferta del cargador, confirmará electrónicamente a éste su recepción, comunicándole, además, los datos descriptivos de la mercancía que coinciden con los que generalmente contienen en los conocimientos de embarque tradicionales. El porteador emitirá el mismo mensaje al Registro central, en el que el cargador aparecerá registrado como el tenedor del *Bolero Bill of Lading*. De esta forma, si el cargador desea trasmitir las mercancías durante la operación de traslado, deberá ponerlo en conocimiento del Registro central comunicándole la identidad del nuevo tenedor[157].

Tras la celebración del contrato de transporte entre cargador y porteador, se crea el *Bolero bill of Landing*, el cual, gracias al juego de una serie de roles creados contractualmente y asignados a diferentes personas, está bajo la titularidad en cada momento de una de ellas. Este documento está integrado por el mensaje para su creación y la información relativa al mismo, y asociada con él, pasa a ser almacenada y a figurar en el registro, siendo el registro lo relevante para determinar la titularidad del acuerdo contractual de los usuarios del sistema. El *Bolero Bill of Landing* implica un reconocimiento por parte del transportista de que las mercancías han sido cargadas a bordo o al menos recibidas para embarque, y de la celebración y los términos del contrato de transporte, pudiendo introducir, al igual que en los conocimientos emitidos en papel, reservas relativas a las mercancías recibidas.

1.3.3.3.3. La seguridad

A fin de ofrecer a los usuarios una adecuada protección contra la posible comisión de fraudes o intromisiones no autorizadas, el sistema BOLERO ha recurrido a la firma digital.

[157] MARTÍN CASTRO. Mª P.: "Documentación electrónica del contrato de transporte", en *Régimen jurídico de internet* (coord. Cremades, J.; Fernández-Ordóñez, M. A; Illescas, R), Madrid, 2002, pág. 630.

El sistema BOLERO justifica este uso en la importancia de la autenticidad, es decir, la capacidad de atribuir confiablemente un documento a su firmante con certeza que el documento se ha mantenido intacto desde que fue firmado. Se dice que, para que el documento firmado en papel pueda ser considerado como equivalente, el documento electrónico debe estar firmado digitalmente; es decir, la firma digital debe ser verificada por la clave pública contenida en un certificado fiable.

Ante esto, cada usuario debe aceptar que un mensaje firmado o una parte extraída de un mensaje firmado digitalmente serán admisibles ante cualquier tribunal como prueba del mensaje o parte del mismo. En caso de que un escrito firmado digitalmente sea requerido por otra parte, la copia presentada por el usuario que BOLERO ha autenticado, deberá ser aceptada por el usuario o por cualquier otro usuario como prueba. Así mismo, si hay una discrepancia entre el registro de cualquier usuario y la copia autenticada por BOLERO, dicha copia autenticada prevalecerá; si se rompiera con lo establecido en las *Rulebook* podría conllevar una acción disciplinaria por parte de la *Bolero Association Ldt*.

1.3.3.3.4. Bolero bill of landing

Es el modelo de conocimiento de embarque electrónico creado por BOLERO que pretende reproducir las funciones propias de los conocimientos de embarque emitidos sobre el papel de tal modo que pueda alcanzarse una eficacia comercial similar a la que tradicionalmente ha correspondido a los documentos de transporte. De esta forma, puede decirse que es el equivalente del conocimiento de embarque convencional[158].

El sistema BOLERO toma como suyo el principio de equivalencia funcional, instaurado por la Ley Modelo sobre Comercio Electrónico. Sin embargo, se pretende ir un poco más allá; es decir, pretende que, además de una equiparación entre el documento en papel y el documento electrónico otorgue una equivalencia económica y jurídica.

[158] MARTÍN CASTRO. Mª P.: "Documentación electrónica del contrato de transporte", en *Régimen jurídico de internet* (coord. Cremades, J.; Fernández-Ordóñez, M. A; Illescas, R), Madrid, 2002, pág. 630.

Con ello, lo que pretende es crear un instrumento que proporcione a los usuarios las ventajas derivadas del comercio electrónico, pero sin que el empleo de las nuevas formas de representación influya negativamente en la protección de los usuarios del sistema, para esto intenta reconducir los principios que informan la tutela del adquirente de los títulos valores al ámbito de la documentación electrónica.

CAPÍTULO SEGUNDO: NOCIONES GENERALES

2.1. Comercio tradicional y comercio electrónico

Una de las áreas problemáticas identificadas en el derecho es la incidencia de las nuevas tecnologías en las instituciones jurídicas; particularmente, la problemática que se suscita alrededor de las transacciones electrónicas.

El cambio tecnológico[159] plantea retos de actualización de los regímenes jurídicos nacionales e internacionales, de modo que puedan responder eficazmente a las exigencias planteadas por la creciente globalización[160] de los asuntos; pues es indudable que los avances tecnológicos, en materia de intercambio electrónico de datos, han propiciado el desarrollo de esta tendencia en todos los órdenes, lo que implica realizar las adecuaciones, en los regímenes, que sean necesarias para que estén acordes con las transformaciones que han tenido lugar en la organización social, económica y empresarial; a nivel mundial, regional, nacional y local.

El desarrollo de las tecnologías de la información ha hecho que los intercambios de bienes y servicios crezcan, simplificando y creando nuevas formas de comercio, desarrollando otra modalidad comercial además de la tradicional de hacer negocios: el comercio electrónico.

El uso comercial de Internet ha hecho que el comercio electrónico se presente como algo accesible a todos, provocando un incremento considerable de las transacciones electrónicas. Estas transacciones vienen a realizarse tanto en el ámbito público como privado y en el ámbito nacional e internacional. De esta manera, el comercio electrónico se ha abierto paso en el comercio tradicional, lo que ha permitido

[159] COLOMBIA: Sentencia de la Corte Constitucional C-662 del 8 de junio de 2000, de 8 de junio de 2000 (Expediente D-2693).

[160] RODRÍGUEZ BENOT, A.; YBARRA BORES, A.: "La determinación del ordenamiento aplicable a los contratos internacionales en un mercado globalizado: la experiencia europea", Congreso Internacional de Derecho Mercantil, Instituto de Investigaciones Jurídicas de la UNAM, del 8 al 10 de marzo de 2006, pág. 347 y ss.
Disponible en: http://www.institutodederechomercantil.org/wp-content/uploads/determinacion-del-ordenamiento-contratos-_rodriguez_ybarra.pdf (última visita: 6/6/2014).

agilizar el intercambio de bienes tangibles e intangibles a la vez que permite hacerlo de una forma más económica[161].

El intercambio de bienes produce no solo en un contexto nacional sino también internacional, lo que hace que los Estados incorporen en sus ordenamientos jurídicos estructuras legales; es decir, normas que permitan hacer efectivo este intercambio y que contribuyan, de manera significativa, al establecimiento de relaciones económicas internacionales armoniosas[162], para, por un lado, dar confianza a sus ciudadanos; por otro, tratar de subsanar cualquier obstáculo.

Si bien, la primera expresión del comercio electrónico surgió en los años ochenta a través del denominado intercambio electrónico de información o EDI (*Electronic Data Interchange*) que, en su vertiente comercial, consistía en la realización de transacciones comerciales de forma automatizada; con el intercambio, en formato normalizado, de órdenes de compra, venta y pago realizadas de ordenador a ordenador, dentro de las comunidades sectoriales, y, generalmente, a través de redes cerradas cuyo uso, previo pago, era proporcionado por los correspondientes proveedores de servicios[163].

Actualmente, el *World Wide Web* (WWW) y el correo electrónico tienen también un papel importante en el comercio electrónico como instrumentos de difusión de la información comercial y como medio de realización de las transacciones electrónicas de forma prácticamente interactiva y on-line, en el caso de la WWW, o a través de procedimientos de almacenamiento y reenvío de mensajes a través de los denominados agentes de transferencias de mensajes, en el caso del correo electrónico. Este nuevo contexto del comercio electrónico, basado en Internet, es conocido como comercio electrónico abierto y se caracteriza por ser un comercio sin necesidad de acuerdos bilaterales previamente negociados y entre partes que no necesariamente mantienen relaciones estables. En este acercamiento, podemos decir que el comercio electrónico es la metodología moderna para hacer negocios, la cual detecta la necesidad de las

[161] MARTÍNEZ NADAL, A.: "Comentarios sobre la regulación de la firma electrónica", *Partida doble*, núm. 106, 1999, págs. 14-33.
[162] CNUDMI/UNCITRAL: *Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, 1999, Exposición de motivos.
[163] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, pág. 29 y ss.

empresas, comerciantes y consumidores de reducir costos, mejorar la calidad de los bienes y servicios y mejorar el tiempo de entrega de los bienes y servicios. Por ello, el comercio electrónico debemos entenderlo no como una tecnología, sino como el uso de la tecnología para mejorar la forma de llevar a cabo las nuevas formas de negocios[164].

De esta forma, se han desarrollado normas jurídicas nacionales tendentes a tratar de: eliminar posibles obstáculos comerciales, reafirmar los derechos de las partes para decidir sobre los medios tecnológicos apropiados para autenticar las transacciones, garantizar la defensa de las partes, otorgar a las tecnologías y proveedores un trato no discriminatorio de terceros países y proteger a los consumidores.

Siguiendo al Prof. Illescas Ortiz[165], podemos decir que las normas jurídicas han otorgado una estructura propia al comercio electrónico. Son identificables los siguientes elementos, que pueden ser agrupados en dos apartados:

a. Elementos objetivos: que no necesariamente son materiales. Estos elementos son:

    1. El mensaje de datos.

    2. La norma técnica de estructuración.

    3. La firma electrónica.

    4. Los sistemas de información.

    5. Las redes de transmisión de datos.

[164] RICÓN CARDENAS, E.*: Manual de Comercio Electrónico y de Internet*, Bogotá, 2006, págs. 27 y ss.
[165] ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, págs. 65 y ss.

b. Elementos subjetivos: se comprenden en el mismo los distintos sujetos destinatarios de los mandatos y privilegios legales así como de los derechos y obligaciones contractualmente adquiridos en el marco jurídico del comercio electrónico. Estos son:

1. El iniciador o firmante del mensaje de datos.

2. El destinatario del mensaje de datos.

3. Los intermediarios y proveedores de servicios de certificación de firma electrónica o autoridad de certificación.

Con esta estructura se puede realizar una tarea de determinación y definición de cada uno de los elementos principales involucrados en la transacción electrónica, a la vez que se podrían tratar los múltiples problemas derivados de la dificultad de aplicar los diferentes conceptos y las categorías jurídicas.

Nosotros nos centraremos en la firma electrónica por su importancia; pues, en ella, se centran todos los fundamentos, para dar al comercio electrónico, las soluciones necesarias a fin de mitigar los riesgos e incertidumbres inherentes a las transacciones por medios electrónicos, que permitirían hablar de un comercio electrónico seguro.

2.2. Firma manuscrita y firma electrónica

Es frecuente, en nuestra actual organización social, la utilización de la firma en documentos tan dispares como pueden ser una simple nota, una carta, un cheque o un contrato. Incluso personas con dificultad de cualquier índole, para leer o escribir, aprendan a plasmar su firma en un documento. A veces, en último extremo, cuando alguien no puede estampar su firma, se recurre a la huella digital[166].

[166] MADRID PARRA, A.: "La identificación electrónica", *Revista de la Contratación Electrónica*, Abril, 2001, núm. º 15, págs. 3 – 60.

De esta forma, si acudimos al Diccionario de la Real Academia Española [167] define la firma como "Nombre y apellido, o título, que de una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido", o *para obligarse a lo que en él se dice*.

Es decir, se trata de un signo único que una persona realiza con el fin de identificarse y asumir el acto que signa. La finalidad perseguida, al firmar un documento, es doble[168]:

a) Asumir la autoría del mismo.

b) Adquirir los derechos y obligaciones que de este se desprendan.

Por consiguiente, el uso de la firma se generaliza como medio de atribución de la autoría de una obra, de un contrato, etc. Nuestro Código civil para la perfección de contratos no exige la firma, pero si el consentimiento[169]. Sin embargo, la práctica ha hecho que la firma sea el medio más frecuente y habitual para dar el consentimiento. No se somete a control ni requisitos. Cada sujeto la adopta y utiliza libremente la forma o el signo que mejor le salga[170].

---

[167] REAL ACADEMIA DE LA LENGUA ESPAÑOLA: Diccionario de la lengua española, Madrid, 2001.
Disponible en: http://www.rae.es/recursos/diccionarios/drae (última visita: 7/4/2014).

[168] ORTEGADÍAZ, J. F.: *La firma y el Contrato de Certificación Electrónico*, Pamplona, 2008, pág. 36.

[169] De esta forma, en España se ha adoptado la regla de la libertad de forma para compromisos contractuales en asuntos de derecho privado. Así lo muestra el Artículo 1258 ("Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley") y el Artículo 1278 ("Los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez").

[170] ESPAÑA: Sentencia del Tribunal Supremo (Contencioso-Administrativo) de 3 noviembre 1997 (RJ 1997\8251), que nos dice que "La firma es el trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse con lo que en ellos se dice. Aunque la firma puede quedar reducida, sólo, a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor".

Nuestro Tribunal Supremo[171] se ha referido a la firma como "la firma es el trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse con lo que en ellos se dice. Aunque la firma puede quedar reducida, solo, a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor". De este modo, se pone de relieve la regla de la libertad de forma para los compromisos contractuales, con alguna excepción.

Por otra parte, en el derecho anglosajón, una firma es todo nombre o símbolo utilizado por una parte con la intención de constituya una rúbrica. El paradigma de la firma es el nombre del firmante, escrito de su puño y letra en un documento de papel. Sin embargo, no es el único tipo de firma posible, una firma puede ser una marca, un nombre impreso, etc. siempre que se aporten pruebas de que demuestren que tal marca o nombre impreso fue puesto por la persona que dice haber firmado o que dicho firma sea reconocida y así lo haga saber la persona que ha otorgado la autoridad para consignarla en el documento concreto[172]. Los requisitos legales de la firma, como condición para la validez de determinados actos en foros de derecho anglosajón, figuran en la Ley contra el Fraude británica y sus versiones en otros países[173].

Con el nacimiento del comercio electrónico surge la necesidad de desarrollar una serie de elementos interrelacionados entre sí, que puedan brindar fiabilidad práctica y una idoneidad comercial a los usuarios (ya se trate de empresas, consumidores o Administraciones) en toda transacción a realizar. En este sentido, se debe brindar a los usuarios un valor agregado que dé certidumbre jurídica al comercio electrónico, dando pie a la formulación de legislación, que regule la utilización de técnicas modernas de autenticación y mejorare las ya existentes, en relación con las garantías jurídicas requeridas en las relaciones documentadas en papel. Se trata de buscar un modelo que facilite la utilización de las firmas electrónicas, de manera que sea aceptable para

[171] Sentencia del Tribunal Supremo (Contencioso-Administrativo) de 3 de Noviembre de 1997, Recurso número 532/1995 (RJ 1997\8251).
[172] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electró*nicas, Viena, 2009, párr. 3 y 4.
[173] MASON, S.: *Electronic signature in Law,* Cambridge, 2012, págs.5 y 6.

Estados con distintos ordenamientos jurídicos, sociales y económicos podría contribuir al fomento de relaciones económicas armoniosas en el plano internacional[174].

De igual manera que la firma manuscrita constituye un medio convenido para imputar derechos y obligaciones nacidos de los datos contenidos en papel, esta forma de firmar no es la única, pues hay otros mecanismos que constituyen trazados gráficos y también conceden autoría y obligación. Con esto, nos estamos refiriendo a: códigos, sellos, huellas, etc.; es decir, a todos "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos"[175].

Se trata de ofrecer mecanismos que puedan cumplir las mismas funciones que las firmas manuscritas en un entorno electrónico, proporcionando equivalentes funcionales de tales firmas y otros tipos de mecanismos de autenticación empleados para el soporte papel.

2.3. Firma electrónica y firma digital

Todo documento electrónico es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido por medio de cifras, signos, códigos de barras, claves, nombre mecanografiado o datos biométricos, de manera que es posible identificar a los agentes materiales, que son sujetos de derechos y obligaciones en la transacción.

En la medida en que nos vamos adentrando en el uso de la firma electrónica, observamos que la firma del documento electrónico es un procedimiento novedoso, de complejidad técnica, pero de uso sencillo, que nada tiene que ver con la firma manuscrita, si bien puede cumplir las mismas funciones[176].

---

[174] CNUDMI/UNCITRAL: *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno (2001)*, Nueva York, 2002.
[175] Artículo 2,a) de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno (2001).
[176] MADRID PARRA, A.: "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil***,** núm.34, 2001.

El uso de la firma electrónica no se encuentra limitado a sectores concretos ni a personas o entidades determinadas; pues, puede utilizarse tanto en el sector privado como en el sector particular, bien entre particulares o bien entre Administraciones[177].

En el sector privado su uso puede estar vinculado a cuestiones relacionadas con la vida privada por vía electrónica, entre empresas y consumidores, entre empresa y empresa o incluso entre consumidores particulares. En el sector público el uso de la firma electrónica puede estar relacionado con actuaciones habituales como renovación de documentos oficiales, solicitud de prestaciones sociales a organismos competentes por medios electrónicos, remisión electrónica de documentos a la Seguridad Social, declaraciones de la renta, presentación de documentos en procedimientos administrativos, etc.[178]

Por consiguiente, a través de la firma electrónica, el firmante trata de declarar la autoría de un documento electrónico determinado, de manera que dé fiabilidad a terceros de que dicho documento que se le va a imputar al firmante le vincula jurídicamente[179]; es decir, tiene consecuencias jurídicas en caso de incumplimiento y, asimismo, dicho documento les llega integro e inalterado.

Dentro del desarrollo ordinario de la relación que vincula a las partes intervinientes, tanto el comerciante como sus clientes, tratan de consolidar un vínculo de confianza, que está ligado, entre otras cosas, a forma en la que se perfecciona el acuerdo determinado y se maneja la información; es decir, se trata de identificar a la persona que realiza la transacción, pues, para generar confianza, es necesario estar seguro de que fue él (el firmante), y no otro, el autor del documento y de la autenticación de la transacción, en lo que se refiere a la intencionalidad de dar a conocer la voluntad de aparecer ligada al acto, que ella misma ha creado[180].

---

[177] ROSSELLÓ MORENO, R.: *Comercio electrónico y la protección de los consumidores*, Barcelona, 2001, pág. 43.
[178] MADRID PARRA, A.: "La identificación electrónica*", Revista de la Contratación Electrónica*, Abril, 2001, núm. 15, págs. 3 – 60.
[179] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica*, Madrid, 2009, pág.
[180] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE (2001)*, párr. 29 y ss.

Nos encontramos ante una necesidad que repercute sobre la transmisión de datos relativos al contrato electrónico por ausencia de elementos físicos, que contribuyan a la identificación de los participantes. A este respecto, hay legisladores que han optado por conferir la presunción de que cumplen tal función, cuando se utiliza el método de infraestructura de clave pública con determinados requisitos, sobre la base de un sistema de criptografía asimétrica, lo que se conoce como firma digital.

La defensa en el uso de esta tecnología se fundamenta en la necesidad de proteger la información. La seguridad de la información es determinante para evitar la vulnerabilidad de la misma, por ello, la importancia a fin de garantizar su disponibilidad (el acceso legítimo a la información en los términos fijados por su titular), su confidencialidad (que excluye la puesta a disposición de personas o usos no autorizados) y su integridad (referida a su no modificación)[181].

Se trata de que, mediante la utilización de la criptografía de clave asimétrica, cualquier persona que desee firmar un documento tenga a su disposición un par de claves (pública y clave privada) que se correspondan matemáticamente, de tal manera que lo que se firma con una clave (privada del remitente), sólo se puede verificar con la correspondiente clave asociada (pública del remitente). Con ello, debemos tener en cuenta que lo relevante no es que solo se pueda verificar con la clave pública, sino que tal verificación asegura quién es el firmante (el tenedor único de la clave privada).

La finalidad de la firma digital es garantizar la autenticación, el no repudio y la integridad: en este sentido la firma digital puede asegurar la procedencia de la firma y que no se niegue más tarde su existencia. Para conseguir la integridad del documento será necesaria la aplicación de una función matemática concreta denominada *hash* a la información que va a ser enviada. Tras su aplicación se obtiene un resumen, compendio, *digest* o huella digital. Las características fundamentales de la función de hash estriban en su carácter único[182].

[181] DE MIGUEL ASENSIO, P. A.: *Derecho privado de internet*, Madrid, 2002, pág. 383.
[182] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, pág.

Con esto, observamos que los términos "Firma Electrónica" y "Firma Digital" parecen iguales pero no lo son. La expresión "Firma Electrónica" nace con el comercio electrónico y se enmarca en la necesidad de asegurar la identidad del emisor y del receptor de la comunicación; la "Firma Digital" se enmarca en la necesidad de dar seguridad, otorgando a la firma diversos requisitos de forma y de fondo en los distintos ordenamientos jurídicos[183].

2.4. Protección de datos personales

El comercio electrónico y la información que se deriva de la transacción, identificados los sujetos mediante la firma electrónica, presenta una gran relevancia para el posterior tratamiento que se produce en el almacenamiento, manipulación o transmisión de cara al tratamiento de datos de carácter personal.

La importancia que tiene la información, en el funcionamiento de la sociedad de la información, ha dado origen a la creación de varias formas de registro de datos gracias a la interconexión de equipos informáticos y de bases de datos, la descentralización y crecimiento de redes, y, especialmente, por el hecho de reunir, en un instrumento interactivo y multidireccional, el mayor número de usuarios que puede englobar un medio. Los avances en Internet han obligado a aumentar la capacidad de los ordenadores, permitiendo el desarrollo de nuevas vías de negocio así como de nuevas formas de Marketing; al mismo tiempo, se han puesto de manifiesto también vulnerabilidades y faltas de seguridad importantes.

A esto hay que añadir el carácter transnacional de Internet, con los problemas de jurisdicción y competencia judicial que dificultan el control y aplicación de gran parte de las garantías legales que pretenden, de algún modo, regular los contenidos o el flujo de datos a través de la red.

Por ello, no resulta extraño que tanto las instancias públicas como privadas recojan informaciones, bien como fin propio a su actividad o bien para servir de soporte a otras actividades igualmente de naturaleza pública o privada. Esto ocurre con los

[183] CRUZ RIVRO, D.: *Eficacia formal y probatoria de la firma electrónica*, Madrid, 2006, pág. 21 y ss.

sistemas de información y almacenamiento informático que surgen por efecto del funcionamiento de Internet, caracterizándose por un hecho adicional relativo al contenido de los datos electrónicos que se intercambian, pudiendo ser rastreado hasta su origen.

La información que se comparte en Internet deja huella que permite establecer el contenido exacto de la transacción comercial y, además, hace posible rastrear e identificar todo lo que la persona hizo (lugares que visitó, consultó e incluso los productos que consumió). Con solo apretar el teclado de nuestro ordenador se podemos conocer la totalidad de los datos de una persona.

Esta realidad conlleva la necesidad de crear mecanismos de protección que permitan fijar límites acerca de la información que puedan ser conocidas por terceros, garantizando el derecho a la intimidad de quienes realizan una actividad económica o navegan por Internet.

En definitiva, el desafío que se presenta es proteger los derechos y libertades fundamentales, en especial el derecho a la privacidad y el derecho al acceso a información personal (también conocido como *habeas data*[184]) y, al mismo tiempo, estimular el flujo libre y seguro de información dentro y fuera de un país, lo que es esencial para la continua expansión del comercio electrónico, computación en nube y otros servicios web; de esta forma, para abordar el problema de la protección es necesario delimitar el marco legal que pueda dar garantías a los usuarios[185].

Para ello, debemos tener en cuenta que la protección de datos se basa en el derecho de las personas a la privacidad. Sin embargo, el significado de la privacidad y los orígenes del derecho individual a la privacidad pueden variar. En consecuencia, las políticas y leyes que rigen el derecho a la privacidad difieren de un país a otro. Habida cuenta de esta divergencia en el tratamiento del derecho a la privacidad, la legislación

[184] ESPAÑA: Sentencia del Tribunal Constitucional de 292/2000, de 30 de noviembre de 2000 (RTC 2000\292) reconoce "La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4)".

[185] FABIO PIACENZA, D.: "Habeas Data derecho a la información", *AR. Revista de Derecho Informático*, núm.34, 2010, págs. 26 y ss..

que protege el tratamiento de los datos personales puede variar de una región a otra e incluso dentro de una misma región. En términos generales, podemos decir que nos encontramos ante tres sistemas de protección de datos[186]:

a) El sistema europeo: con sistema estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por parte del gobierno y las entidades privadas.

b) El sistema de Estados Unidos permite que los sectores económicos regulen los datos personales recabados por organizaciones privadas y la regulación estatal de los datos recabados por el Estado.

c) El sistema de protección de los países miembros de la Organización de Estados Americanos (OEA), han elaborado mecanismos de protección de datos basados en el concepto de *habeas data*, el cual es un derecho constitucional de carácter jurisdiccional destinado a la salvaguarda de la libertad de la persona, en cuanto a su esfera informática. Esto implica el derecho de cualquier persona para acudir ante una instancia jurisdiccional, en el caso de que sus datos personales, o los de su grupo familiar, se hayan visto modificados, afectados o alterados, para que estos sean rectificados o suprimidos, y por ello, se concrete la reparación efectiva de tal vulneración[187].

[186] CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA): *Principios y Recomendaciones preliminares sobre la protección de datos (la protección de datos personales)*, Washington, 2011, pág. 4.
Disponible en: http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf (última visita: 31/5/2014).

[187] ROSARIO RODRÍGUEZ, M. F.: "La protección de datos personales entre particulares: esbozos de un esquema de regulación y protección en México", *Derecho comparado de la información*, 2012, núm.20, págs. 107 – 126.

La OEA, en junio de 2011, presentó un documento[188] sobre los "Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales", preparado de conformidad con la resolución AG/RES. 2514[189].

Este documentos recoge un detallado informe sobre los principios y recomendaciones sobre la protección de datos, como son: los requisitos para el procesamiento, propósitos y circunstancias para el procesamiento, responsabilidad del procesador, terceros procesadores, transferencias transfronterizas, *habeas data* y cumplimiento. Además, el texto recomienda medidas proactivas y de cooperación en la materia mediante la cual los Estados deben crear programas de capacitación, educación y conciencia pública para fomentar la comprensión de la legislación, los procedimientos y los derechos en materia de protección de los datos personales; procedimientos operativos normalizados para los controladores de datos a fin de prevenir, detectar y contener las posibles violaciones de la seguridad; también para promover cooperación entre autoridades nacionales, encargadas de la protección de datos personales a nivel nacional e internacional para favorecer esta protección.

En Estados Unidos[190], la privacidad aparece como un concepto amplio relacionado con la libertad dentro de una esfera íntima. Su construcción es fundamentalmente jurisprudencial hasta que, en 1974, empezaron a promulgarse algunas normas, basadas en la presión y preocupación de los ciudadanos con el abuso y las exigencias del mercado. El derecho a la privacidad está destinado a proteger los sentimientos y la sensibilidad de las personas y no su propiedad o intereses pecuniarios. Existe la costumbre judicial de proteger a las partes que así lo soliciten por seudónimos. Asimismo, es posible perder parte del derecho a la privacidad, para ello se han establecido dos categorías de personas: las voluntariamente públicas (aquellas que se han expuesto ante la mirada del público por su actividad, ya sean músicos, actores, etc.

[188] CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA): Principios y Recomendaciones preliminares sobre la protección de datos (la protección de datos personales), Washington, 2011, pág. 4.
Disponible en: http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf (última visita: 31/5/2014).

[189] CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA): *Ley Modelo Interamericana sobre acceso a la información pública*, l8 de junio de 2010.
Disponible en: http://www.oas.org/dil/esp/AG-RES_2607-2010.pdf (última visita: 31/5/2014).

[190] GREGORIO DE GRACIA, C.: "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América latina", en *Transparentar al Estado: la experiencia mexicana de acceso a la información* (Dirs. Cocha Cantí, H.; López Ayllón, S.; Tacher Epelstein, L.). México DF, pág. 312 y ss.

y por ello el público puede tener un interés legítimo en obtener información que puede ser tan amplia que incluiría aspectos que para otras sería privados); y las involuntariamente públicas (aquellas que no han buscado atención del público pero que han sido noticia como resultado de su participación en algún hecho notorio).

En Europa, para abordar la protección es necesario delimitar el marco legal. Nos situaremos en España, cuyo origen legal de la protección de datos de carácter personal de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, que fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) que traspone la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. La LOPD puede ser completada con el establecimiento de códigos tipo permitidos por la ley (Artículo 32) contemplados como códigos deontológicos o de buenas prácticas profesionales.

En fecha de 25 de enero de 2012 se ha aprobado una propuesta de Reglamento[191] relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)[192], que viene a modificar la normativa vigente hasta ahora, realizando una revisión de conceptos en materia de privacidad. El futuro Reglamento introduce definiciones como: brecha en la seguridad de los datos, información genética, información biométrica, datos de salud, establecimiento principal, representante, empresa, grupos de empresas y normas vinculantes corporativas.

Es importante recordar que la Carta de los Derechos Fundamentales reconoce una serie de derechos personales civiles, políticos, económicos y sociales de los ciudadanos

[191] Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES (última visita 24/10/2014).

[192] En fecha de 22 de noviembre se ha emitió el Proyecto de Resolución Legislativa del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).
Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES (última visita: 34/10/2014).

y residentes de la Unión Europea que se consagran en la legislación comunitaria[193], entre los que se encuentra el respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones (Artículo 7) y el derecho a la protección de los datos de carácter personal que le conciernan (Artículo 8). Lo que supone una protección mayor a la que se realiza en los ordenamientos de ámbito anglosajón.

En virtud de la normativa en vigor, la LOPD en su Artículo 1 nos dice que "esta Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar", y en su Artículo 3,a) nos dice que son datos personales: "cualquier información concerniente a personas físicas identificadas o identificables". Se nos está indicando, dentro de una definición amplia, dos elementos esenciales: la información y el sujeto. De esta forma, tendrá la condición de dato personal el nombre, apellido, número del DNI o afiliación de una persona, imágenes, sonidos y voces, con la única limitación de que esos datos resulten suficientes para identificar a su titular. No se discrimina por tanto información alguna, cualquier detalle o pormenor de una persona física que permita identificarla, tiene la categoría de dato de carácter personal[194].

De esta forma, se está hablando de unos datos de pertenencia a una persona que individualmente pueden configurar un perfil determinado sobre una o varias características del individuo que tiene derecho a exigir que permanezcan en su esfera íntima, y por tanto, en un entorno protegido[195].

Es por ello que, por ejemplo, cuando se utiliza un ordenador para acceder a la red, la IP del ordenador (número de identificación denominado Internet Protocol), dato accesible para los demás que acceden a la red, no encuentra resguardo en la ley; pues, con este número se está identificando a una máquina no a una persona. Ahora bien, si

[193] CARTA DE LOS DERECHOS FUNDAMENTALES RECONOCE UNA SERIE DE DERECHOS PERSONALES, CIVILES, POLÍTICOS, ECONÓMICOS Y SOCIALES DE LOS CIUDADANOS Y RESIDENTES DE LA UE, CONSAGRÁNDOLOS EN LA LEGISLACIÓN COMUNITARIA: Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33501_es.htm (última visita: 6/5/2014).

[194] BELEN QUINTANA, A.: "Capítulo I: Introducción" en *La protección de datos en la gestión de empresas* (Dir. Marzo Portera, A. y Ramos Suarez, F. Mª), Navarra, 2004, pág. 36 y ss.

[195] DAVARA RODRÍGUEZ, M. A.: *La protección de datos en Europa*, Madrid, 1998, págs. 19 y ss.

cuenta con información adicional que permita establecer un nexo entre ese número y una persona si habrá dado el salto que permite entrar en la consideración de dato personal[196]. Téngase en cuenta que no es necesario llegar a celebrar contratos para que se aporten datos personales, basta con comenzar a moverse por la red para que se genere un tráfico de datos personal

Por otra parte, cuando hablamos de correo electrónico habrá que ver si identifica a una persona o no. Si identifica no hay duda de que será objeto de protección, si no identifica la agencia concluyó que también se encuentra protegido puesto que el sujeto es identificable mediante la consulta del servidor en que se gestione dicho dominio. Este sentido se ha pronunciado la Audiencia Nacional[197] al decir que "la dirección de correo electrónico de la que es titular una persona física, constituye una información que le concierne, le afecta y que forma parte del ámbito de su privacidad".

Además, mediante correo electrónico se puede realizar una contratación electrónica, aunque también por más medios, para lo cual han de identificarse las partes. Así, cuando se recaban datos personales se debe informar de lo dispuesto en el artículo 5 de la citada Ley Orgánica, según el cual: "1) Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. 2) Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior".

[196] MADRID PARRA, A.: "Contratación electrónica y protección de datos personales", *Revista de la Contratación Electrónica*, 2008, núm. 94, págs. 3 – 85.
[197] ESPAÑA: Sentencia Audiencia Nacional (Contencioso-Administrativo) de 15 enero 2011(RJCA 2011\2).

En consecuencia, cuando se recaban datos personales (entre ellos la firma) debe informarse de los expuesto anteriormente. Por tanto, teniendo en cuenta que la firma del contrato presupone su aceptación y si los datos se usan para el exclusivo cumplimiento del mismo, informándose debidamente al titular de los datos, se cumpliría la normativa de protección de datos. Si la firma digitalizada se usa para otros fines distintos, se podría estar infringiendo dicha normativa.

2.5. Protección de los consumidores

Al tratar la protección de datos hemos querido fijar una realidad marcada en el ordenamiento jurídico, tratando de detectar peculiaridades que también afectan a la firma electrónica. De esta manera, hemos querido resaltar que la protección de datos siempre será aplicable con independencia de los datos que se generen o no a partir de la contratación electrónica de la que es parte importante la firma electrónica.

Tras la protección de datos nos situamos en la corriente que nos lleva a la protección del consumidor, vertiente comercial de la protección de datos, que es de lo que nos vamos a ocupar en las siguientes líneas. En la protección de los consumidores es necesario observar la realidad y el ordenamiento jurídico existente.

Los avances de la humanidad en los campos científicos y tecnológicos siempre han planteado retos al derecho. Tienen efectos directos en la estructura política y económica de la sociedad que, de acuerdo con su grado de incidencia en el tráfico jurídico, en la distribución de bienes y servicios y en el ejercicio de los derechos fundamentales de la persona, demandan diferentes respuestas del ordenamiento jurídico.

De esta forma, en la existencia de una nueva red mundial de comunicaciones y vías de circulación de la información accesible, fácil y directa al ciudadano para múltiples propósitos; entre ellos, la prestación de servicios y el ejercicio de actividades de naturaleza financiera o comercial a escala global, no es una realidad inocua. Esta realidad puede regularse de diferentes maneras, el legislador no puede optar por expedir normas contrarias a su carácter, a veces, más notorio: su internacionalidad.

En este nuevo escenario tecnológico, en desarrollo constante, la protección de los derechos del consumidor, persona física o jurídica, cobra un significado crucial, pues se trata de garantías esenciales para generar confianza. En Internet puede haber realidad virtual, pero eso no significa que los derechos también lo sean: se trata de garantías expresas que deben quedar reconocidas en el ciberespacio. Nadie puede sostener que los usuarios, por tratarse de Internet, pueden sufrir mengua de sus derechos.

Ante esto, observamos que la principal consecuencia del comercio electrónico, en general, es el contrato electrónico. Su clasificación depende de los sujetos que interactúan en el mismo, como empresas, consumidores y las administraciones públicas. Por lo tanto tenemos[198]:

a) Comercio de empresa a empresa (*Business to Business*, B2B).

b) Comercio de empresa a consumidor (*Business to Consumer*, B2C).

c) Comercio de empresa a administración pública (*Business to Administrations*, B2A)[199].

Estos son los principales tipos de comercio electrónico en relación con los sujetos, pero nada impide que se puedan formar más relaciones entre agentes[200]:

a) De consumidor a consumidor (*Consumer to Consumer*, C2C)[201].

[198] GONZÁLEZ MARTÍN, N.: "Comercio electrónico y la protección del consumidor: acercamiento al contexto mexicano" en *Comentarios actuales al derecho mercantil internacional* (Dirs. Calvo Caravaca, A. L. y Areal Ludeña, S.), Madrid, 2005, págs. 616 y ss.

[199] Teniendo en cuenta que el comercio electrónico, basado en el tratamiento electrónico y la transmisión de datos, abarca actividades muy diversas que van desde el intercambio de bienes y servicios a la entrega en línea de información digital, pasando por la transferencia electrónica de fondos, la actividad bursátil, la contratación pública. (COMISIÓN EUROPEA: *Comunicación de la Comisión de 18 de abril de 1997: Una iniciativa europea en el sector del comercio electrónico (COM (97)157 final– no publicada en el Diario Oficial)*, Bruselas, 16 de abril de 1997, pág. 8).

[200] LA Comisión Europea nos dice que el comercio electrónico cubre "todo tipo de negocio, transacción administrativa o intercambio de información que utilice cualquier tecnología de la información y las comunicaciones. Desde la perspectiva empresarial, va desde la simple compra diaria hasta los complejos sistemas que completan el ciclo comercial" (COMISIÓN EUROPEA: *Libro blanco del comercio (COM (1999) 6 final)*, Bruselas, 27 de enero de 1999, pág. 12).

[201] Nos referimos a la realización de transacciones entre consumidores, procesos de compraventa de un

b) De consumidor a administración pública (*Consumer to Administrations*, C2A)[202].

c) De consumidor a empresa (*Consumer to Business*, C2B)[203]

Buena parte de la efectividad del derecho depende del hecho de que: tanto las partes entre quienes se perfeccione un acuerdo sobre un objeto específico, como las autoridades encargadas de ejercer la inspección de tales transacciones, cuenten con la información necesaria que permita tener certeza sobre la naturaleza de dichos actos y los efectos que puedan tener.

El objetivo básico de cualquier normativa reguladora de la contratación electrónica es establecer, en relación con esos aspectos, un marco jurídico equivalente a la normativa típica de la contratación de consumo en el marco físico tradicional. En ese marco normativo es clave hacer posible una tutela eficaz de los consumidores que puede resultar determinante para el desarrollo del comercio electrónico, lastrado por la incertidumbre[204].

El principal problema que nos encontramos es que la localización del proveedor se sitúe en el extranjero, lo que puede ser fuente de inseguridad, por si fuera el caso de que las cosas no salen como el consumidor espera y tiene que interponer una reclamación. De esta forma, una transacción internacional nos lleva a una protección internacional del consumidor.

---

determinado producto sin que exista la necesidad de un intermediario destacando, por ejemplo, las subastas online.

[202] Nos referimos a situaciones donde los usuarios interactúan con la Administración Tributaria o con la Seguridad Social a efectos realizar transacciones, presentar transacciones, etc.

[203] Nos referimos a modelos en los que el consumidor es la parte activa de la relación comercial. Este modelo de transacciones, que no se da normalmente, es fruto de una negociación entre el consumidor y empresario. Este modelo, principalmente, se refiere a una intermediación entre consumidores y empresarios, en las que se contacta con proveedores que responde a la petición del consumidor, que es quién establece o decide el precio máximo a pagar por un servicio o un producto (encontramos ejemplos como: http://www.priceline.com o http://www.ebolution.com). No obstante, en la práctica, podemos ver que el negocio no plantea desde los consumidores, sino desde plataformas empresariales, lo que nos permitiría hablar de un B2C encubierto (un ejemplo, http://www.agrupate.com).

[204] MIGUEL ASENCIO, P. A.: "Mercado global y protección de los consumidores" en *Consumidores y usuarios ante las nuevas tecnologías* (Coord. COTINO HUESO, L.), Valencia, 2008, pág. 155.

La protección de los consumidores se lleva a cabo por un entramado de normas, que combina elementos de derecho privado y de derecho público. La heterogeneidad del contenido, configuración y eficacia de la normativa de los consumidores, según el país, se halla fuertemente influenciado por condicionantes, tales como: las preferencias sociales, la tradición política y cultural, el contexto jurídico, el criterio ideológico y de política económica, así como factores que incluyen el nivel de industrialización y desarrollo económico.

Esta circunstancia se corresponde con la falta de estándares internacionales comunes, pues a nivel internacional la cooperación intergubernamental se limita a día de hoy a mecanismos incipientes de cooperación e intercambio de información entre autoridades de alcance muy limitado o en instrumentos no vinculantes[205].

En efecto, a nivel convencional, en materia contractual, ya sea respecto a la ley aplicable o a la jurisdicción, encontramos instrumentos internacionales. Sin embargo, excluyen de su ámbito de aplicación los contratos celebrados con consumidores. Tal es el caso, por ejemplo, de la Convención de Naciones Unidas sobre Contratos de Compraventa Internacional de Mercaderías (1980), que en su Artículo 2,a) establece que no se aplicará a las compraventas de mercaderías adquiridas para uso personal, familiar o doméstico, salvo que el vendedor, en cualquier momento antes de la celebración del contrato o en el momento de su celebración, no hubiera tenido ni debería haber tenido conocimiento de que las mercaderías se compraban para ese uso; o la Convención de Naciones Unidas sobre la Utilización de la Comunicaciones Electrónicas en los Contratos Internacionales Electrónicos (2005), que también, en su Artículo 2,a), excluye de su ámbito de aplicación los contratos concluidos con fines personales, familiares o domésticos.

Sin embrago, hay que destacar la formulación de Directrices de las Naciones Unidas para la Protección del Consumidor, adoptadas por la Cuarta Conferencia de Naciones Unidas encargada de examinar todos los aspectos del conjunto de principios y normas equitativos convenidos multilateralmente para el control de prácticas comerciales restrictivas, celebrada en Ginebra los días 25 a 29 de septiembre de 2000.

[205] MIGUEL ASENCIO, P. A.: "Mercado global y protección de los consumidores" en *Consumidores y usuarios ante las nuevas tecnologías* (Coord. COTINO HUESO, L.), Valencia, 2008, pág. 158.

Estas directrices para la protección del consumidor tienen como objetivo[206]:

a) Ayudar a los países a lograr o mantener una protección adecuada de sus habitantes en calidad de consumidores.

b) Facilitar las modalidades de producción y distribución que respondan a las necesidades y los deseos de los consumidores.

c) Instar a quienes se ocupan de la producción de bienes y servicios y de su distribución a los consumidores a que adopten estrictas normas éticas de conducta.

d) Ayudar a los países a poner freno a las prácticas abusivas comerciales abusivas de todas las empresas, a nivel nacional e internacional, que perjudiquen a los consumidores.

e) Facilitar la creación de grupos independientes de defensa de los consumidores.

f) Promover el establecimiento de condiciones que den a los consumidores una mayor selección a precios más bajos.

g) Promover un consumo sostenible.

Estas directrices son aplicables tanto a los bienes y servicios producidos en un país como a los importados, debiendo velarse para que, al aplicar cualquier

[206] UNCTAD: Conferencia de las Naciones Unidas sobre comercio y desarrollo: Directrices de las Naciones Unidas para la protección del consumidor (ampliadas en 1999), Nueva York y Ginebra, 2001, pág. 1.
Disponible en: http://unctad.org/es/Docs/poditcclpm21.sp.pdf (última visita: 6/6/2014).

procedimiento o reglamento para la protección del consumidor no se conviertan en barreras para el comercio internacional y que sean compatibles con las obligaciones del comercio internacional. De esta manera, se viene a decir que los gobiernos deben ocuparse especialmente de: a) establecer, examinar, mantener o fortalecer, según proceda, los mecanismos para el intercambio de información relativa a políticas y medidas nacionales en la esfera de la protección del consumidor; b) cooperar o alentar la cooperación en la aplicación de las políticas de protección del consumidor para conseguir mejores resultados en el marco de los recursos existentes; c) cooperar para mejorar las condiciones en los que los productos esenciales se ofrezcan a los consumidores, prestando atención a los precios y a la calidad.

Asimismo, la OCDE, en abril de 1998, elaboró unas Directrices para la Protección del Consumidor en el contexto del comercio electrónico[207], cuyo objetivo es garantizar la protección de los consumidores a través de la obligación de información apropiada relativa a las actividades, bienes y servicios objeto del comercio electrónico, a las operaciones en línea y sobre los procedimientos eficaces de resolución. En este sentido, recomienda a los países tener en cuenta la vulnerabilidad del consumidor en Internet, para ofrecer una protección jurídica transparente, equivalente y funcional, semejante a la que se otorga, comúnmente, en otras formas de comercio.

Posteriormente, en 2003, la OCDE publicó nuevas Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, que tienen por objeto que los países miembros trabajen en el desarrollo de un marco que permita una cooperación más cercana, rápida y eficiente entre sus agencias encargadas de vigilar el cumplimiento de las leyes de protección al consumidor, para ello se propone: que establezcan un sistema nacional para combatir prácticas comerciales transfronterizas fraudulentas y engañosas en contra de los consumidores; promuevan un mayor apoyo mutuo en materia de notificaciones, intercambio de información e investigación; mejoren la capacidad de proteger a los consumidores extranjeros de proveedores nacionales dedicados a las prácticas comerciales fraudulentas y engañosas; mejoren la capacidad de proteger a los

[207] ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS: Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, París, 2004.

consumidores nacionales de proveedores extranjeros dedicados a las prácticas comerciales fraudulentas y engañosas; consideren formas para asegurar el resarcimiento efectivo a los consumidores víctimas; e incluya la cooperación con las entidades del sector privado pertinentes[208].

2.5.1. Defensa regional de los consumidores

Siguiendo, de manera especial, las Directrices de Naciones Unidas para la protección del consumidor en las que se recomendaba a los gobiernos de ocuparse, especialmente en un contexto regional o subregional, de fortalecer vínculos nacionales en la esfera de protección del consumidor[209] nos permite encontramos con algunos casos concretos.

2.5.1.1. Tratado de Libre Comercio entre México – Canadá – Estados Unidos

El Tratado de Libre Comercio de América del Norte (TLCAN)[210] es un acuerdo que suscribieron Canadá, Estados Unidos y México en 1994 para establecer progresivamente la apertura de los mercados a través del libre comercio de productos, bienes y servicios en la región.

Dentro del texto de Tratado de Libre Comercio de Norteamérica, podemos encontrar disposiciones directamente relacionadas con la protección de los consumidores, concretamente en el Artículo 915, dentro del Capítulo IX ("Medidas relativas a la normalización"), Parte Tercera ("Barreras técnicas al comercio"), que viene a decir que: "norma internacional significa una medida relativa a normalización, u otro alineamiento o recomendación, adoptada por un organismo internacional de

[208] ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS: Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, París, 2004, pág. 7.
Disponible en: http://www.oecd.org/sti/consumer/34012151.pdf (última visita: 6/6/2014)
[209] UNCTAD: Conferencia de las Naciones Unidas sobre comercio y desarrollo: Directrices de las Naciones Unidas para la protección del consumidor (ampliadas en 1999), Nueva York y Ginebra, 2001, pág. 17.
Disponible en: http://unctad.org/es/Docs/poditcclpm21.sp.pdf (última visita: 6/6/2014).
[210] Tratado de Libre Comercio de América del Norte (TLCAN).
Disponible en: http://www.economia.gob.mx/comunidad-negocios/comercio-exterior/tlc-acuerdos/tlcan (última visita: 6/6/2014)

normalización y puesta a disposición del público pudiendo evidenciarse ciertos elementos: a) seguridad; b) la protección de la vida o la salud humana, animal o vegetal, del medio ambiente y de los consumidores, incluidos asuntos relativos a la calidad e identidad de bienes o servicios; y c) el desarrollo sostenible". De esta forma, prevé la elaboración de normas profesionales relativas a la protección del consumidor.

2.5.1.2. MERCOSUR

Dentro de la estructura institucional de MERCOSUR, considerando la importancia de la defensa del consumidor, se ha creado, en el ámbito de la Comisión de Comercio del MERCOSUR, un Comité Técnico encargado de elaborar un Proyecto de Reglamento Común para la Defensa del Consumidor del MERCOSUR[211]. Si bien dicho Proyecto no ha podido ser concretado aún a día de hoy; no obstante, existen algunas normas y declaraciones dignas de ser citadas en esta materia:

a) Declaración CMC N° 10/96 Protocolo de Santa María sobre Jurisdicción)/ Internacional en Materia de Relaciones de Consumo.

b) Resolución GMC N° 42/98 sobre Garantía Contractual.

c) Declaración Presidencial de Derechos Fundamentales de los Consumidores del MERCOSUR.

d) Acuerdo Interinstitucional de Entendimiento entre los Organismos de Defensa del Consumidor de los Estados Partes del MERCOSUR para la Defensa del Consumidor Visitante.

Actualmente, y de acuerdo a su Programa de Trabajo 2004, el CT 7 trabaja, entre otros temas, en un Programa de Intercambio entre Organismos de Defensa del

[211] Proyecto de Reglamento Común para la Defensa del Consumidor del MERCOSUR: Disponible en: http://www.comercio.gob.ar/web/index.php?pag=284&btn=163 (última visita: 6/6/2014).

Consumidor de los Estados Partes, en la creación de un sitio electrónico sobre temas de defensa del consumidor y en varios proyectos que corresponden a la armonización de materias que formarán parte del Reglamento Común que constituye la aspiración fundamental de este Comité. La mencionada normativa y las actividades encaradas recientemente, implican la firme voluntad de los Estados Partes de impulsar el tema en el ámbito del bloque.

2.5.1.3. Unión Europea

Como hemos visto hasta ahora, la protección del consumidor supone un elemento importante en el comercio electrónico, en el que comerciantes contratan con comerciantes establecidos en países extranjeros.

En la Unión Europea está dimensión internacional tiene un tratamiento importante, que ha venido a realizarse a través de normas que se ocupan de la defensa del consumidor en el ámbito comunitario con una doble vertiente: respecto a la defensa de consumidores respecto a comerciantes establecidos dentro de la Unión europea dentro la propia Unión y defensa de consumidores con respecto a comerciantes establecidos en terceros países.

Esto se manifiesta, por un lado, con la Directiva 2000/31/CE, sobre comercio electrónico, establece que establece que completará el ordenamiento jurídico comunitario aplicable a los servicios de la sociedad de la información, sin perjuicio del nivel de protección, en particular, de la salud pública y de los intereses del consumidor fijados tanto en los instrumentos comunitarios como en las legislaciones nacionales que los desarrollan. Por tanto, el régimen de protección singular de la contratación electrónica se superpone al régimen jurídico de la protección del consumidor, por lo que al contrato electrónico celebrado vía electrónica le resulta de aplicación toda la normativa de consumidores prevista en el ordenamiento jurídico nacional y comunitarios[212].

[212] PLAZA PENADÉS, J.: "Marco general de la protección del consumidor en la contratación electrónica" en *Consumidores y usuarios ante las nuevas tecnologías* (Coord. COTINO HUESO, L.), Valencia, 2008, pág. 54; en este sentido, véase también la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras

Por un lado, la actuación del legislador europeo ha ido encaminada, en materia de consumo, a la armonización de las legislaciones de los Estados miembros, adoptando una serie de Directivas, que ha terminado con la aprobación de la Directiva 2011/83/UE, del Parlamento y del Consejo, de 25 de octubre de 2011, sobre derecho de los consumidores, por la que se modifican la Directiva 93/13/CEE, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores y la Directiva 1999/44/CE, de 25 de mayo de 1999, sobre determinados aspectos de la venta y las garantías de los bienes de consumo, y se derogan la Directiva 85/577/CEE de 20 de diciembre de 1985, referente a la protección de los consumidores en el caso de contratos negociados fuera de los establecimientos comerciales y la Directiva 97/7/CE, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia[213].

Por otro lado, se manifiesta, a través de la adopción de reglas específicas sobre competencia judicial internacional en los contratos de consumo (Artículos 15 a 17 del Reglamento 44/2001), la incorporación de un régimen específico sobre ley aplicable a los contratos de consumo (Artículo 5 del Convenio de Roma de 1980). La aplicación de este entramado de protección a las actividades de comercio electrónico es, en la actualidad, fuente significativa de controversia e interés, pues la interpretación de algunas de estas normas, al entorno electrónico, está siendo debatida, hoy[214].

Además de la mencionada normativa, la jurisprudencia del TJCE ha desarrollado una importante labor en materia de protección de los consumidores, estableciendo claramente cuál es el criterio de interpretación para determinar si una reglamentación de

---

leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre (BOE nº. 76, de 28 de marzo; corrección de errores en BOE nº. 117, de 14 de mayo) que traspone la Directiva 2011/83 (publicada con fecha de 22 de noviembre de 2011) e incide directamente en la regulación del comercio electrónico B2C (BOE-A-2014-3329) (BOE-A-2014-5107).
Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-3329 (última visita: 9/12/2014).

[213] DIRECTIVA 2011/83/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de octubre de 2011 sobre los derechos de los consumidores.
Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:ES:PDF (última visita: 6/6/2014).

[214] DE MIGUEL ASENCIO, P. A.: "Mercado global y protección de los consumidores" en *Consumidores y usuarios ante las nuevas tecnologías* (Coord. COTINO HUESO, L.), Valencia, 2008, pág. 159.

la Unión Europea establece un elevado nivel de protección de los derechos de los consumidores[215].

[215] LARRAZABAL BASAÑEZ, S.: "La protección de los consumidores en la carta de los Derechos Fundamentales de la Unión Europea", *Jado boletín de la Academia Vasca de Derecho*, 2011, nº 22, págs. 21 – 35.

CAPÍTULO TERCERO: LA IDENTIDAD ELECTRÓNICA

3.1. Identificación electrónica

Teniendo presente el Diccionario de la Real Academia Española, debemos entender por identificación la "acción y efecto de identificar o identificarse", y por identificar la "acción de hacer que dos o más cosas se parezcan y se consideren una misma, o la acción de reconocer si una persona es la misma que se supone o que se busca o incluso dar los datos personales necesarios para ser reconocido". Estas definiciones nos llevan necesariamente a la identidad, recogida en el diccionario de la RAE, como, la "colección dinámica de todos los atributos relacionados con un individuo específico, entidad u objeto"[216].

De esta forma, en la vida diaria, decimos que la identidad es lo que permite a las personas físicas o jurídicas distinguirse, posibilitando que se vincule una información a una persona en concreto y, a la vez, realizar un manejo eficaz y seguro de los datos específicos del individuo. Esto hace de la identidad un componente clave en todas las transacciones económicas, sociales y administrativas.

Si en el mundo real, una identidad se establece a partir de un conjunto de características vinculadas a la propia persona, como puede ser, por ejemplo, el nombre, altura, fecha de nacimiento, número de identificación fiscal, domicilio, etc. que en suma constituyen un DNI, es decir, una identificación nacional. En el mundo en línea[217], la identidad se puede atribuir al conjunto de rasgos que caracterizan al individuo o a un colectivo en un medio de transmisión electrónico. A la persona se le atribuye una huella de un fichero, que se transforma a partir de unos datos de longitud variable que dan lugar a una serie de caracteres de longitud fija, que son únicos a partir de los datos de entrada; es decir, no existe otra entrada distinta que dé por resultado el mismo hash, huella o Digest. Dicho en otras palabras, la identidad electrónica es un conjunto de

[216] REAL ACADEMIA DE LA LENGUA ESPAÑOLA: *Diccionario de la lengua* española, Madrid, 2001.
Disponible en: http://www.rae.es/recursos/diccionarios/drae (última visita: 7/4/2014).
[217] STALLINGS, W.: *Fundamento de seguridad en Redes: Aplicaciones y Estándares*, Madrid, 2010, págs. 9 y ss.

informaciones y datos relevantes para una persona, física o jurídica, que se almacenan y se trasmiten a través de los sistemas electrónicos y se utiliza con el fin de identificar a una persona.

La necesidad de vincular la información y su manejo únicamente con quien la emite hace esencial para numerosas interacciones diferentes: una infraestructura organizativa (gestión de la identidad) y una infraestructura técnica (sistemas de gestión de identidad), para desarrollar, definir, designar, administrar y especificar los niveles de autorización, asignando roles y atributos de identidad relacionados con grupos específicos de personas, como los empleados, clientes, pacientes o simplemente ciudadanos.

Por ello, la identidad importa mucho y su significado plantea grandes dificultades en las transacciones transfronterizas. Lo veremos, por ejemplo, en el debate en torno a los sistemas de gestión, respecto a las tarjetas de identificación electrónicas, donde los problemas reales que se sustentan respecto a la identidad nacional y su impacto en la sociedad, por la combinación que realizan respecto de la identificación en el mundo real y del mundo en línea, si bien en ambos ámbitos se presentan como documentos de identificación nacionales y, a la vez, ante la sociedad estatal con las mismas vulnerabilidades respecto a la sustracción de la identidad con todo lo que ello supone, especialmente respecto a la inseguridad; pues, los ciudadanos ven en la red probabilidad mayor en que la amenaza se materialice.

En este contexto, es necesario analizar los marcos legales y el tratamiento que hacen de la identidad, con el fin de evaluar las bases de la gestión correcta de los riesgos, de los impactos debidos a posibles brechas de seguridad y de las construcción de las medidas de salvaguardia que, en un principio, se han creado, considerando éstas para minimizar o anular los riesgos.

3.1.1. La identidad electrónica como elemento esencial de la firma electrónica: actuaciones internacionales

La determinación de la identidad del signatario es uno de los requisitos para crear una firma electrónica válida. La CNUDMI en la Ley Modelo sobre Comercio Electrónico de 1996, en su Artículo 7, en relación con el mensaje de datos, recoge una definición genérica y amplia de firma electrónica, que viene a decir que: la firma electrónica es un método o técnica para llevar a cabo la identificación del autor de un mensaje electrónico.

Posteriormente, en la Ley Modelo sobre Firma Electrónica en 2001, de una forma más acotada nos dice, en su Artículo 2,a), que las firmas electrónicas son "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos".

De esta forma, al igual que la Ley Modelo sobre Comercio Electrónico, establece como rasgo definitorio de la firma electrónica su capacidad para identificar al firmante y mostrar su capacidad respecto del mensaje. Esta aprobación no debe entenderse en sentido estricto; es decir, no respecto a la emisión del consentimiento para quedar jurídicamente obligado; pues de lo contrario, estaríamos hablando de la autenticación de la transacción. Por ello, lo que se pretende es establecer un nexo de unión entre la información del mensaje de datos y la persona que lo emite, con independencia de que se produzcan o no, consecuencias jurídicas concretas [218].

Lo que, en nuestra opinión, realiza la Ley Modelo es inducir al establecimiento de un proceso que sirva para verificar alguno de los rasgos que permiten identificar al individuo o a la colectividad, de la misma forma que, por ejemplo, en el caso de una conversación telefónica, ese proceso de reconocimiento de la voz del individuo que se encuentra al otro lado de la línea, permite identificar al individuo inconscientemente.

Además, con esta definición, recogida por la Ley Modelo sobre Firma Electrónica recogida en el Artículo 7 de la Ley Modelo sobre Comercio Electrónico, se pretende que esta sea lo suficientemente amplia como para abarcar todas las firmas electrónicas

[218] MADRID PARRA, A*:* "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista de Derecho Patrimonial,* año 2003 – 2, número 11, págs. 31 – 63.

existentes en la actualidad y las que puedan utilizarse en el futuro, con independencia de la tecnología o los métodos empleados para su creación, en equivalencia con las firmas manuscritas.

Para completar la definición dada por la Ley Modelo sobre Firma Electrónica debemos acudir al Artículo 6, que en su párrafo segundo, nos dice acerca de la identificación del sujeto, como persona que parte con la intención de vincularse o autentificar un documento, "es esencial su identificación" como parte, para diferenciarlo de otra persona que pueda utilizar su nombre u otros datos. Ante esto nace la necesidad de usar un método fiable a la luz de las circunstancias, lo que nos llevaría a entrar en la autenticación, puesto que estamos ante un método fiable a la luz de las circunstancias, en cuanto que hablamos de la determinación incluida en el párrafo 1 del Artículo 6, lo hacemos constituyendo un método centrado en la fiabilidad de la firma electrónica, en el sentido de que la utilización de esa firma ha de surtir efectos jurídicos equivalentes a la firma manuscrita[219].

Este contexto, planteado por las Leyes Modelo, que ha sido seguido en mayor o menor medida por la mayoría de los Estados, ha favorecido la promulgación de leyes que han facilitado el reconocimiento jurídico del comercio electrónico y de la firma electrónica Se ha conseguido un mínimo común en todos los ordenamientos jurídicos existentes, lo que ha inspirado a la CNUDMI, entre otros motivos, "considerando que los problemas creados por la incertidumbre en cuanto al valor jurídico de las comunicaciones electrónicas en los contratos internacionales constituyen un obstáculo para el comercio internacional", a adoptar la Convención de Naciones Unidas sobre Comunicaciones Electrónicas en los Contratos Internacionales de 2005.

Centrándonos en la identificación, esta Convención en su Artículo 9, que tiene por enunciado "Requisitos de forma", trata de manera separada tres elementos: "escrito", "firma" y original", debiendo ampliarse sus conceptos, en especial, en cuanto a la firma y al original, con el fin de evitar cualquier posibilidad de solapamiento entre ellos.

[219] MADRID PARRA, A: "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista de derecho patrimonial*, año 2003 – 2, núm. 11, págs. 31 – 63.

En el apartado tercero se recoge la "firma", que tiene la única finalidad suprimir los obstáculos que se oponen a la utilización de las firmas electrónicas, pero no influyen en los demás requisitos para la validez de las comunicaciones electrónicas a las que se refieren las firmas electrónicas[220]. En virtud de la Convención, la mera firma de una comunicación electrónica mediante un equivalente funcional de la firma manuscrita no debe conferir, *per se*, validez jurídica a la comunicación electrónica. La validez jurídica de una comunicación electrónica que cumpla los requisitos de firma debe decidirse en virtud de la ley aplicable al margen de la Convención[221].

De esta forma, se viene a decir que, ante la utilización de técnicas electrónicas de autenticación en lugar de las firmas manuscritas y otros procedimientos tradicionales de autenticación, se ha creado la necesidad de establecer un marco jurídico específico que reduzca la incertidumbre sobre los efectos jurídicos que puedan derivar de la utilización de esas técnicas modernas, que la Convención denomina como "firmas electrónicas".

Ante el riesgo de que en los distintos países se legisle de forma dispar sobre las firmas electrónicas, se hace necesario la adopción de reglas básicas, que la Convención las centra en dos[222]:

a) Las funciones básicas de una firma deben desempeñarse mediante un método que determine la identidad del firmante.

b) Que se asegure el nexo entre el firmante y la información.

Por consiguiente, una firma electrónica debe permitir determinar la identidad del firmante e indicar la intención de éste, con respecto a la información consignada en la comunicación electrónica; por otro lado, el método empleado para la identificación debe

[220] OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, págs. 45-88.
[221] CNUDMI/UNCITRAL: *Nota explicativa a de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 156.
[222] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 245.

ser tan fiable como apropiado para los fines para los que se generó la comunicación electrónica.

Esto es así, porque la Convención no trata de determinar equivalentes tecnológicos específicos para determinadas funciones de las firmas manuscritas. En cambio, fija las condiciones generales en las que las comunicaciones electrónicas se considerarán autenticadas con suficiente credibilidad y serán ejecutables aunque existan requisitos de firma, basándose en las dos funciones básicas de la citada firma[223]; el apartado a) del párrafo 3 del Artículo 9, establece el principio por el que, en el marco de las comunicaciones electrónicas, las funciones legales básicas de una firma debe desempeñarse mediante un método, que determine la identidad del iniciador de una comunicación electrónica; a saber, la del autor de un documento y la intención de éste respecto a la información consignada en la comunicación electrónica[224].

En virtud de lo establecido en la Convención, la mera firma de una comunicación electrónica, mediante un equivalente funcional de firma manuscrita, no debe, por sí misma, conferir validez jurídica a la comunicación electrónica; la validez jurídica de una comunicación electrónica que cumpla los requisitos de firma debe decidirse en virtud de la ley aplicable al margen de la Convención[225].

Por otro lado, los apartados cuarto y quinto se refieren al "original", en semejanza a lo recogido en el Artículo 8 de la Ley Modelo de Comercio Electrónico. Se pone de relieve la importancia de la integridad de la información para que mantenga su carácter original y enuncian los criterios a tener en cuenta para evaluar la integridad refiriéndose al registro sistemático de la información, a la garantía de que la información ha sido

[223] OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, págs. 45-88.
[224] CNUDMI/UNCITRAL: *Nota explicativa a de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 154.
[225] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 156.

registrada sin lagunas y a que se hayan protegido los datos frente a toda alteración. Estableciéndose un vínculo entre identidad, originalidad y autenticación[226].

De esta forma, se observa cómo desde la CNUDMI, a través de sus Leyes Modelo y de la Convención, se ve la identidad como un elemento esencial, facilitador del despliegue de los servicios transfronterizos, a la vez que es un elemento clave para el aumento de las actividades económicas empresariales, siendo la identidad electrónica y los servicios de autenticación unos de los aspectos que más preocupa a nivel internacional. Al mismo tiempo que ve la verificación de la identidad como otro requisito decisivo.

Además de la CNUDMI, encontramos numerosos grupos intergubernamentales, Estados, grupos internacionales privados y entidades comerciales que ejercen una gran influencia sobre ellas. Estos han estudian las cuestiones y oportunidades relacionadas con la gestión de la identidad, elaborando normas técnicas y procesos empresariales que buscan nuevas formas de aplicar sistemas de identidad digital viables en los distintos foros internacionales, persiguiendo con empeño el sueño de un mercado electrónico único[227].

Entre los grupos intergubernamentales que trabajan activamente en cuestiones y normas de gestión de la identidad digital, entre los que figuran la OCDE, la Organización Internacional de Normalización (ISO), la Unión Internacional de Telecomunicaciones (UIT) y la Conferencia de la Haya.

Varios proyectos regionales relacionados con la identidad digital se encuentran en marcha en la Unión Europea, entre los que cabe mencionar *PrimeLife* (un proyecto del Séptimo Programa Marco de la Comisión Europea), *Global Identity Networking of Individuals - Support Action* (GINI-SA), STORK (encaminado a establecer una

[226] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 169.

[227] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 3.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

plataforma europea de interoperabilidad de la eID) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Se han establecido algunos sistemas de identidad digital comerciales que funcionan a escala mundial en esferas reducidas. Entre ellos figuran los que administran *Transglobal Secure Collaboration Program* (TSCP) y *CertiPath* para las industrias aeroespacial y de defensa, la *SAFE-BioPharma Association* para la industria biofarmacéutica, IdemTrust26 para el sector financiero, el *CA/Browser Forum27* para los certificados EV-SSL de sitios web y *FiXs - Federation for Identity and Cross-Credentialing Systems* (FiXs). La labor de esos grupos se centra primordialmente en cuestiones relacionadas con normas técnicas y procesos empresariales y no en cuestiones de orden jurídico.

3.1.1.1. Conferencia de la Haya: las e-Apostillas

El uso transfronterizo de documentos firmados se complica con la intervención de alguna autoridad pública, pues las autoridades receptoras de un país extranjero suelen exigir alguna prueba de identidad y autoridad del firmante.

De este modo, con el aumento del tráfico internacional, también lo ha hecho el riesgo de falsificación de documentos públicos que, a menudo, los ciudadanos necesitan presentar para hacer valer en otros países.

Por tradición, los requisitos de presentación de documentos se cumplen por los procedimientos de legalización de estos, a través de los cuales, las firmas que figuren en documentos nacionales, son autenticadas por autoridades diplomáticas para su utilización en el extranjero.

En la relación de los ciudadanos con las Administraciones Públicas, junto con el creciente número de documentos electrónicos emitidos por éstas, ponen de manifiesto la necesidad de adaptar el trámite de la legalización única o Apostilla a la realidad actual de la sociedad de la información.

La legalización de documentos públicos mediante Apostillas se encuentra recogida en el Convenio XII de la Conferencia de la Haya de Derecho Internacional Privado, firmado el 5 de Octubre de 1961, por el que se suprimió la exigencia de legalización de los documentos públicos autorizados en el territorio de un Estado contratante y que deberían ser presentados en el territorio de otro Estado contratante, creando la Apostilla.

La Apostilla[228] es un trámite de legalización único, que consiste en colocar sobre un documento público una apostilla que certifica la autenticidad del documento expedido en otro país, suprimiendo las exigencias de legalización diplomática o consular para los documentos públicos.

Por otro lado, hemos de hacernos eco del Artículo 7 del Convenio[229]. Este Artículo dispone que las autoridades designadas deberán llevar un registro o fichero en el que queden anotadas las Apostillas expedidas, a instancias de cualquier interesado, la autoridad que la haya expedido deberá comprobar, si las anotaciones incluidas en la apostilla se encuentran sujetas a las del registro.

Hoy en día, todo se vincula a temas electrónicos de forma que las nuevas tecnologías forman parte de la sociedad actual y su utilización es un hecho incontestable.

La Comisión Especial sobre el funcionamiento práctico del Convenio sobre la Apostilla, la obtención de pruebas y la notificación, en el establecimiento de una serie

---

[228] Web del Ministerio de Justicia. Disponible en: http://www.mjusticia.gob.es/cs/Satellite/es/1200666550200/Tramite_C/1215326297910/Detalle.html (última visita: 26/3/2014).

[229] Artículo 7 del Convenio de la Conferencia de la Haya Suprimiendo la Exigencia de Legalización de Documentos Públicos Extranjeros dice: "Cada una de las autoridades designadas conforme al artículo 6 deberá llevar un registro o fichero en el que queden anotadas las Apostillas expedidas, indicando:

c) El número de orden y la fecha de la apostilla.
d) El nombre del signatario del documento público y la calidad en que haya actuado o, para los documentos no firmados, la indicación de la autoridad que haya puesto el sello o timbre.

A instancias de cualquier interesado, la autoridad que haya expedido la Apostilla deberá comprobar si las anotaciones incluidas en la Apostilla se ajustan a la del registro o fichero".
Disponible en: http://www.hcch.net/index_es.php?act=conventions.text&cid=41 (última visita: 26/3/2014).

de conclusiones y recomendaciones[230], insistió en que la implantación de la nuevas tecnologías de la información "pueden tener efectos positivos en el funcionamiento del Convenio, de forma señalada en la disminución de los costes y en la mayor eficacia de los procedimientos de expedición y registro de Apostillas".

Teniendo en cuenta el Artículo 3 del Convenio que nos dice que el efecto de una Apostilla es "certificar la autenticidad de la firma, el carácter con el que ha actuado en signatario del documento, y en su caso, la identidad del sello o del timbre que lleva el documento", se recomienda a los Estados partes a que trabajen en el desarrollo de técnicas para generar Apostillas electrónicas teniendo presente la Ley Modelo de Comercio Electrónico y la Ley Modelo de Firma Electrónica, recogiendo los principios sobre los que versa, principalmente, la no discriminación y la equivalencia funcional.

Asimismo, la Conferencia de La Haya de Derecho Internacional Privado en abril de 2006, lanza el *e-Apostille Pilot Program* (e-APP)[231], que prevé: por una parte, la utilización de la tecnología *Adobe Acrobat*, generando un documento PDF que puede ser dotado de una capa de datos XML, cuya utilización favorece el desarrollo de un estándar de datos comunes para las Apostillas electrónicas; por otra, se trabaja en la creación de registros electrónicos mediante un modelo basado en soluciones de código abierto.

Por consiguiente, favorece la utilización de certificados digitales para la firma electrónica de este tipo de Apostillas, lo que asegura la integridad, autentificación y no rechazo; además, de que cualquier persona destinataria de un documento apostillados puede confirmar con garantía el origen de esta línea, introduciendo el número y fecha de la Apostilla. La solicitud realizada genera una respuesta automática mediante la cual se señala una inscripción o no de la Apostilla en cuestión del registro electrónico[232].

---

[230] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Conclusiones y Recomendaciones adoptadas por la Comisión Especial sobre el Funcionamiento práctico de los Convenios sobre Apostilla, la Obtención de Pruebas y la Notificación.*, octubre/noviembre de 2003, párr.7.
Disponible en: http://www.hcch.net/index_es.php?act=publications.details&pid=3121&dtid=2 (última visita: 31/3/2014).

[231] Nueva Zelanda, el 13 de mayo de 2009, ha emitido la primera apostilla electrónica de conformidad con el modelo sugerido en virtud del Programa Piloto de Apostillas electrónicas, siendo la primera emitida en la región de Asía – Pacífico.

[232] RODRÍGUEZ BENOT, A.: "La aplicación de las nuevas tecnologías a la cooperación jurídica internacional: la Apostilla Electrónica" en *Derecho internacional privado – Derecho de la libertad y el*

En el empleo de estas técnicas, se crea un marco jurídico de seguridad, que reduce la incertidumbre con respecto a las posibles consecuencias jurídicas, que pueden derivarse del empleo de las nuevas tecnologías, ofreciéndose un vínculo de seguridad entre la fiabilidad técnica y la eficacia jurídica de la firma documental, fijando un principio de no discriminación entre la información consignada sobre el papel y la información archivada electrónicamente.

Ante el éxito generado por este proyecto, el 14 de Febrero de 2011, se celebró la 1ª Reunión Regional de Proyecto del e-APP para Europa[233] en la que tomaba como ejemplo a España.

España ha promovido la implantación de un sistema de expedición de apostilla electrónica que permite el funcionamiento de un Registro electrónico centralizado de Apostillas electrónicas[234,] así como la emisión de apostillas electrónicas a nivel nacional. En cualquier caso, las apostillas electrónicas se firmarán usando un sistema de firma electrónica avanzada para archivos PDF de acuerdo con la Directiva 1999/93/CE sobre Firmas Electrónicas, lo que implica la aplicación de la Ley 59/2003, 19 de diciembre, de firma electrónica y la Ley 11/2007 de Acceso Electrónico a los Ciudadanos y a los Servicios Públicos.

En noviembre de 2012, la Comisión Especial se citó en La Haya para revisar el funcionamiento práctico del Convenio de La Haya de 5 de octubre de 1961[235], siendo la primera vez que se reunió para dedicarse, exclusivamente, sobre esta cuestión. En esta asamblea la Comisión Especial reconoce el valor de la e-APP como herramienta para incrementar la seguridad y el funcionamiento efectivo del Convenio sobre Apostilla y toma nota con satisfacción de la progresiva implementación del e-APP y de la expansión que ha tenido el uso de la e-Apostilla y la e-registro. Además, aplaude los esfuerzos de un número considerable de Estados contratantes, activamente involucrados

---

respeto mutuo. Ensayos a la memoria de Tatiana B. de Maekelt (Dirs. en Fernández – Arroyo, D.P. y Moreno Rodríguez, J. A.) CEDEP/ASADIP, Asunción, 2010, págs. 649 – 665.

[233] Disponible en: http://www.hcch.net/index_es.php?act=publications.details&pid=5241&dtid=49

[234] Orden JUS/1207/2011, de 4 de mayo, por la que se crea y regula el Registro Electrónico de Apostillas del Ministerio de Justicia y se regula el procedimiento de emisión de apostillas en soporte papel y electrónico.

[235] Disponible en: http://www.hcch.net/index_es.php?act=text.display&tid=37 (última visita: 26/3/2014).

en la implementación de la e-APP, y alienta encarecidamente a los Estados contratantes, que aún no lo hayan hecho, a que consideren su implementación. Con todo ello, pide que se continúe con el intercambio de información entre Estados para la puesta en funcionamiento de la e-APP.

3.1.1.2. Marco jurídico común para la identificación electrónica en Europa: STORK

La Directiva 1999/93/CE sobre firmas electrónicas ha estado en vigor durante más de 13 años. Como veremos en el capítulo siguiente con más detenimiento, la Directiva tiene lagunas importantes que constituyen un freno al uso transfronterizo de la firma electrónica, a la vez se viene demandando por todos los usuarios una mayor seguridad en los servicios electrónicos.

Ante esta demanda se ha desarrollado un nuevo marco jurídico: el Reglamento Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. El origen para su establecimiento, basado en la identificación electrónica, debemos situarlo en el Tratado de Lisboa[236], firmado en esta ciudad, el 13 de diciembre de 2007, que entro en vigor el 1 de diciembre 2009, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, y que, en gran parte, reproduce las innovaciones contenidas en el "fallido" Tratado que establecía una Constitución para Europa.

El Tratado de Lisboa sitúa la libertad, la justicia y la seguridad entre sus prioridades más importantes. Con ello, se quiere poner en práctica políticas en diversos campos: crecimiento económico y competitividad, desarrollo del empleo y las condiciones sociales, aumento de la seguridad personal y colectiva, fomento del medio ambiente y las condiciones sanitarias, desarrollo de la cohesión y la solidaridad entre los Estados miembros, en cuanto a progreso científico y tecnológico, además de mejorar su capacidad de actuación en la escena internacional.

[236] Disponible en: http://europa.eu/lisbon_treaty/full_text/index_es.htm (última visita: 26/3/2014).

Por esto, se dota a la Unión Europea de base jurídica, para trabajar en el establecimiento de un marco jurídico, para la identificación electrónica. De modo más concreto, en el Tratado de Lisboa encontramos tres disposiciones legales que podrían invocarse para sostener la acción legal de la UE en el ámbito de la identificación electrónica, que son[237]:

a) Artículo 77 del Tratado de Funcionamiento de la Unión Europea (TFUE[238]), que recoge la posibilidad de que la UE, en referencia a las políticas de fronteras, asilo, inmigración, etc. pueda establecer, con arreglo a un procedimiento legislativo especial, disposiciones relativas a los pasaportes, documentos de identidad, permisos de residencia o cualquier otro documento asimilado.

b) Artículos 20 a 25 TFUE, en el que se recoge lo que podríamos denominar como el derecho de la ciudadanía europea. En efecto, la ciudadanía de la Unión se añade a la ciudadanía nacional sin sustituirla, lo que presupone la necesidad de crear un sistema de identificación dentro de la zona europea.

c) Artículo 16 TFUE, donde se consagra que el derecho a la protección de datos de carácter personal, afirmando que las comunicaciones electrónicas y la protección de los datos personales se encuentran íntimamente conectadas.

Además, el Artículo 114 TFUE se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. A través de este precepto, se pretende que los ciudadanos, empresas y administraciones puedan beneficiarse del reconocimiento y la aceptación mutua de la identificación, autenticación y la firma electrónica y otros servicios de confianza través de las fronteras

[237] GOMES DE ANDRADE, N. N.: "Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID", *ScienceDirect Review*, vol. 28, núm. 2, 2012, págs. 153 - 162.
[238] Tratado de Funcionamiento de la Unión Europea es resultante del Tratado de Lisboa, que otorga a la Unión Europea competencias sobre "cooperación administrativa".

cuando resulte necesario para el acceso y la realización de procedimientos o transacciones electrónicos[239].

Con este nuevo marco jurídico, a partir de 2010, en la Agenda Digital para Europa[240], aparece una revisión de la Directiva sobre firmas electrónicas, con el fin de proporcionar un marco jurídico para el reconocimiento transfronterizo y la interoperabilidad de los sistemas de autenticación electrónica. Para ello, la Comisión desarrolla una propuesta[241] sobre el reconocimiento mutuo de la identificación y la autenticación electrónicas en toda la UE, en 2012, sobre la base de servicios de autenticación en línea que se ofrecen en todos los Estados miembros.

Así pues, se recoge como un objetivo, el establecimiento de medidas legales para garantizar el reconocimiento mutuo de la e-Identificación (e-ID) y de la autenticación electrónica. Estas medidas se repitieron en las Doce Líneas de Actuación para El Mercado Único de 2012[242]. A estas medidas, se unió el Plan de Acción sobre Administración Electrónica Europea 2011-2015, y las Conclusiones del Consejo, diciendo de ellas que eran necesarias "para garantizar el reconocimiento mutuo de la identificación electrónica y autenticación electrónica en toda la UE". Por último, el Plan de trabajo para la Estabilidad y el Crecimiento, subrayaba estas medidas como clave para el desarrollo de la economía digital.

Una vez establecido el espacio comunitario de competencia, que abarca el campo de la identificación electrónica, la Unión Europea tiene a su disposición toda una amplia gama de diferentes maneras en las que poder intervenir en esta área en particular.

---

[239] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final

[240] COMISIÓN EUROPEA: *Una Agenda Digital para Europa: iniciativas clave (IP/10/581)*, Bruselas, 19 de mayo 2010; COMISIÓN EUROPEA: *Una Agenda Digital para Europa: ¿en qué me beneficia? (MEMO/10/199*), Bruselas, 19 de mayo de 2010; y COMISIÓN EUROPEA: *Agenda Digital: la Comisión esboza un plan de acción para potenciar la prosperidad y el bienestar europeos (MEMO/10/200)*, Bruselas, 19 de mayo de 2010.
Disponibles en: http://europa.eu/rapid/press-release_MEMO-10-200_es.htm (última visita: 23/4/2010).

[241] De esta propuesta resultó el del Parlamento europeo y del Consejo de 23 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, aprobado el 23 de julio de 2014 y publicado en el DOUE el 28 de agosto de 2014.

[242] COMISIÓN EUROPEA: *Doce líneas de actuación para el mercado único de 2012: juntos para un nuevo crecimiento (IP/11/469)*, Bruselas, 13 de abril de 2011.

Por consiguiente, se presenta la opción de optar por hacer una reglamentación uniforme, armonizadora de las legislaciones nacionales, imponiéndoles requisitos de reconocimiento mutuo, pues es consciente de que no se han desarrollo sistemas interoperables de gestión de identidades en Europa. La prueba la encontramos en que la construcción y la realización del mercado único digital ha sido objeto de enfoques jurídicos diferentes y, a menudo, incompatibles en lo que respecta a la protección y gestión de identidades electrónicas[243].

Hasta ahora, habían sido los Estados miembros los que habían tomado la iniciativa, proponiendo los sistemas de identificación a los ciudadanos, así como a los sistemas nacionales de gestión de identidades, siendo muchos países los que han desarrollado e implantado (o están en proceso de hacerlo) tarjetas de identidad electrónicas (Alemania, España, Italia, entre otros); dado que la UE no había hecho uso del poder concedido en el Tratado de Lisboa.

Por esta razón, surge la necesidad de armonizar la amplia y diversa gama de leyes nacionales sobre e-ID, como un imperativo del mercado interno, lo que ha justificado, a nuestro juicio, la aprobación del Reglamento 910/2014 relativo a la identificación electrónica y servicios para las transacciones electrónicas en el mercado interior.

El Reglamento trata de conseguir un entorno regulador previsible, con la finalidad de alcanzar unas interacciones electrónicas seguras entre las empresas, los ciudadanos y los poderes públicos, para aumentar la eficacia de los servicios en línea, tanto del sector público como del privado.

La identificación electrónica viene definida en el Artículo 3,1 como "el proceso de utilizar los datos de identificación de una persona en forma electrónica que representan inequívocamente a una persona física o jurídica". Los medios de identificación podrán ser unidades materiales o inmateriales que posean los datos antes referidos y se utilicen para el acceso a servicios en línea.

[243] CRAIG, P.: "Constituciones, constitucionalismo y la Unión Europea", en *La encrucijada constitucional de la Unión Europea* (Dir. García de Enterría), Madrid, 2002, pp. 229-265.

Como hemos dicho, la mayoría de los Estados habían introducido algún tipo de régimen de identificación electrónica. Estos sistemas son diferentes entre sí, ya que hasta hoy no existía una base jurídica común, capaz de obligar a los Estados a utilizar una identificación interoperable transfronteriza.

Así, el Artículo 6 establece el reconocimiento y la aceptación mutua de los medios de identificación electrónica. El citado Artículo presenta como objetivo, el establecer un reconocimiento armonizado de los sistemas de identificación electrónica entre los Estados miembros de la UE.

Precisamente, donde se requiera una identificación electrónica y una autenticación, en virtud de la legislación o la práctica administrativa nacional, para acceder al servicio en línea, éste debe ser accesible para todas las personas, ya sean físicas o jurídicas, que utilizan medios de identificación electrónica expedidos en otro Estado miembro y siempre que, estos datos, estén incluidos en una lista publicada por la Comisión (Artículo 6,1 *in fine*).

Sin embargo, no es obligatorio, para los Estados miembros, registrar sus sistemas de identificación electrónica; es decir, no obliga a notificar sistemas de identificación, sino que obliga a los Estados a reconocer y aceptar las identificaciones electrónicas notificadas en los servicios en línea, cuando sea necesaria la identificación electrónica a nivel nacional. Se espera que muchos los que la lleven a cabo[244]. Está claro que el Reglamento aporta seguridad jurídica, gracias al principio de reconocimiento y aceptación recíproca, por el que los Estados miembros deben aceptar las identificaciones electrónicas nacionales que hayan sido notificadas oficialmente a la Comisión.

Mismamente, se puede apreciar que la formulación del Artículo 6 no coincide exactamente con la intención del Reglamento, pues, si observamos el Considerando 14 del éste dice: "Deben establecerse en el presente Reglamento ciertas condiciones en relación con qué medios de identificación electrónica tienen que reconocerse y cómo deben notificarse los sistemas. Esto contribuiría a que cada Estado miembro adquiera la

[244] Comunicado de Prensa de la Comisión Europea, Bruselas, 4 de junio de 2012.

confianza necesaria en los sistemas de identificación electrónica de los demás y a que se reconozcan mutuamente los medios de identificación electrónica de los sistemas notificados. Debe aplicarse el principio de reconocimiento mutuo si el sistema de identificación electrónica del Estado miembro que efectúa la notificación cumple las condiciones de notificación y esta se ha publicado en el Diario Oficial de la Unión Europea. Sin embargo, el principio de reconocimiento mutuo debe referirse únicamente a la autenticación a efectos de un servicio en línea. El acceso a estos servicios en línea y su prestación final al solicitante deben estar estrechamente vinculados al derecho a recibir dichos servicios en las condiciones fijadas por la legislación nacional"; y del Considerando 15 *ab initio*: "La obligación de reconocer los medios de identificación electrónica debe referirse únicamente a los medios cuyo nivel de seguridad de la identidad corresponde a un nivel igual o superior al exigido para el servicio en línea de que se trate".

Si el uso transfronterizo de los medios de identificación electrónica, al amparo de un régimen notificado, exige que los Estados cooperen para ofrecer interoperabilidad técnica, está claro que se quiere evitar especificaciones técnicas. Sin embargo, el Reglamento reconoce, implícitamente, que es inevitable imponer requisitos técnicos al usuario, pues estas vienen prescritas intrínsecamente en el dispositivo propio del usuario; por lo que, ya se está reconociendo, en nuestra opinión, una inaplicación del precepto mencionado.

Por otro lado, el Artículo 6 es imposible de aplicar en la práctica, pues ello supone que, una biblioteca pública, por ejemplo, a través de un lector de tarjetas requiera autenticación con el fin de ampliar el plazo por el que presta el libro a través de la web, debe adaptar su aplicación web con el fin de hacerla accesible a toda Europa[245]**.** Además, hemos de tener en cuenta, que de forma inmediata no se aplicará; pues no se pueden destruir las tarjetas identificativas ya emitidas por los propios Estados, además, la cesión de soberanía que supone este, es algo a lo que no muchos Estados están dispuestos (por ejemplo, Reino Unido).

[245] JOS DUMORTIER, J.; VANEZANDE, N.: "Trust in the proposed EU regulation on trust services?" *Computer& Law & Security Review*, Vol. 28, núm. 5, octubre, 2012, p. 568 – 576.

Otro aspecto importante es la responsabilidad, que contrae el Estado miembro, en el Artículo 7,1-d) y f) en relación con el Artículo 11, es la responsabilidad de la atribución inequívoca de los datos de identificación de la persona, física o jurídica; es decir, que los datos de identificación atribuidos a la persona no estén vinculados a ninguna otra, y de la autenticación; o sea, la posibilidad de comprobar la validez de los datos de identificación electrónica. Esta responsabilidad no incluye aspectos del proceso de identificación o cualquier otra transacción que requiera identificación[246].

En este contexto surge STORK[247]. STORK se inició, en 2008, con el objetivo de proporcionar un marco de interoperabilidad transfronteriza para el reconocimiento mutuo del DNI electrónico en toda Europa, estableciendo una base sólida para la interoperabilidad[248].

STORK lo podemos situar dentro del Artículo 6 del Reglamento, en cuanto a la obligación de reconocer los medios de identificación electrónica debe referirse únicamente a los medios cuyo nivel de seguridad de la identidad corresponde a un nivel igual o superior al exigido para el servicio en línea de que se trate. Además, la obligación habrá de aplicarse, únicamente, cuando el organismo del sector público en cuestión emplee el nivel de seguridad sustancial o alto en lo tocante al acceso a dicho servicio en línea. Los Estados miembros deberán tener la posibilidad, con arreglo al Derecho de la Unión, de reconocer medios de identificación electrónica con niveles más bajos de certeza de la identidad[249]. El nivel de seguridad depende del grado de confianza que aporte este medio de identificación electrónica sobre la identidad pretendida o declarada por una persona, teniendo en cuenta los procedimientos técnicos, actividades de gestión y controles aplicados[250].

---

[246] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final.

[247] El Reglamento de identificación electrónica que favorecerá el uso de la infraestructura del proyecto STORK 2.0. La regulación sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior (eIDAS), que entró en vigor el 1 de julio de 2014, pretende desarrollar la interoperabilidad y el uso de la identificación electrónica y los servicios de confianza. Su objetivo es eliminar las barreras que dificultan las transacciones electrónicas nacionales y transfronterizas, dándoles la misma validez legal que los procesos basados en el papel. El Reglamento también incluye un refuerzo de la legislación vigente de la Unión Europea en relación con la firma electrónica.

[248] TAUBER, A; KUSTOR, P KARNING, B: "Cross border certified electronic mailing: A European perspective" *Computer&Law Security Review*, febrero, 2013, núm. 1, vol. 29, págs.28 – 39.

[249] Considerando 15 del Reglamento.

[250] Considerando 16 del Reglamento.

Es un proyecto que tiene como fin establecer una Plataforma Europea de Interoperabilidad de Identificación Electrónica que permita a los ciudadanos establecer nuevas relaciones electrónicas de carácter transfronterizo, con tan sólo presentar su identificación electrónica nacional.

La autenticación transfronteriza del usuario para tales relaciones son aplicadas y probadas por STORK a través de cinco planes piloto, que utilizan los servicios gubernamentales existentes en los Estados miembros.

Se espera que, con el tiempo, los proveedores de servicios adicionales se conecten a la plataforma, para poder aumentar el número de servicios transfronterizos a disposición de los ciudadanos europeos. En el futuro, una empresa podría conseguir el reembolso de sus impuestos u obtener ensayos universitarios sin presencia física, todo lo que necesitaría, para tener acceso a estos servicios, sería introducir sus datos a través de su identificación electrónica nacional y obtendría las garantías exigidas de autenticación de su gobierno.

Este enfoque está centrado en la privacidad del usuario, que siempre tiene el control de los datos que está enviando, y en la garantía del papel que desempeña la plataforma STORK: la identificación del usuario que se encuentra en una sesión con un proveedor de servicios, que envía sus datos a este servicio. Mientras que, el proveedor de servicios puede solicitar diversos datos, el usuario siempre controlará los datos remite. El consentimiento explícito del propietario de los datos, el usuario, siempre se requerirá antes de que sus datos sean enviados al proveedor de servicios.

A través de la UE, los Estados reconocerán mutuamente sus esquemas de identificación electrónica. De esta forma, la identificación electrónica emitida por un Estado participante se puede utilizar para acceder a todos los portales incluidos, lo que puede facilitar la interoperabilidad transfronteriza de los sistemas de identificación.

3.1.1.3. American Bar Association (ABA): la identidad federada

Ante la necesidad de abordar, de manera integral, las cuestiones jurídicas planteadas por la gestión de la identidad, la *American Bar Association*, en 2009, constituyó un grupo de trabajo denominado *Identity Management Legal Task Force*[251], que tiene la misión abordar las cuestiones jurídicas relacionadas con la gestión de identidad federada y desarrollar modelos para este tipo de sistemas.

Este grupo de trabajo intenta hacer frente a los asuntos legales a los que se enfrentan todos los participantes en los procesos de gestión de identidades federadas, siendo sus principales objetivos[252]:

a) Identificar y analizar las cuestiones jurídicas que se plantean en relación con el desarrollo y el uso de los sistemas de gestión de identidades federadas.

b) Identificar y evaluar los modelos jurídicos apropiados para tratar estos temas.

c) Desarrollar los términos del modelo y de los contratos que pueden ser utilizados por las distintas partes participantes en el sistema.

La identidad federada es una respuesta a la gestión de la identidad, integrada por personas jurídicas, en su papel de custodio de sus identidades digitales. Se trata, pues, de un modelo que permite a las empresas, con varias tecnologías, normas y casos diferentes de uso, compartir sus aplicaciones para permitir a las personas que utilicen los mismos credenciales de acceso u otra información de identificación personal, a través de dominios de seguridad. De esta forma, se presenta, como objetivo principal, permitir a los usuarios, registrados en un determinado dominio, acceder a la información de otros dominios, sin tener que dar ninguna información adicional.

[251] Identity Management Legal Task Force:
Disponible en: http://apps.americanbar.org/dch/committee.cfm?com=CL320041 (última visita: 21/4/2014).
[252] ABA IDENTITY MANAGEMENT LEGAL TASK FORCE: *Meeting report ABA Identity Management Legal Task Force*, Londres, 10 – 11 diciembre, 2012.

En un modelo federado[253] se encuentran involucrados sujetos: un usuario o individuo, persona que está siendo identificada; un proveedor de identidad, entidad que identifica al usuario y hace una afirmación con respecto a la identidad de éste y del tercero de confianza; y la parte de confianza, el tercero que depende de que esas afirmaciones de identidad sean ciertas, con el propósito de conceder el acceso a los servicios o recursos que proporciona. Esto permite a una organización confiar en afirmaciones de identidad procedentes de otras organizaciones.

Un ejemplo conocido de un proceso federado de gestión de la identidad es la forma en que actualmente se expiden y utilizan las licencias de conducir. Esas licencias, expedidas por una entidad gubernamental, las utilizan diversas partes receptoras no relacionadas entre sí para verificar los atributos de identidad del titular de la licencia. En los servicios en línea de sistema de identidad federado[254], un ejemplo lo encontramos en los cajeros automáticos. En una transacción típica en un cajero automático una persona que tenga una cuenta en el banco A puede utilizar la credencial de identidad que le ha expedido su propio banco (la tarjeta de cajero) para retirar dinero en efectivo en un cajero operado por el banco B (con el que el interesado no tiene ninguna vinculación). Para dar curso a la transacción, a pesar de que no exista una vinculación de esa índole, el banco B se pone en contacto con el banco A través de la red de cajeros automáticos para determinar si la persona es un cliente autorizado del banco A, hacer que el banco A autentique la identidad del cliente (o se determine si utilizó la contraseña correcta) y para obtener de ese banco determinada información sobre la identidad relacionada con el cliente (por ejemplo, si en la cuenta hay fondos suficientes que respalden el retiro de

[253] SMEDINGHOFF, T. J.: *American Bar Association Identity Management Legal Task Force Meeting*, 10 – 12 diciembre, 2012.
Disponible en: http://meetings.abanet.org/webupload/commupload/CL320041/relatedresources/02-TS-Intro-and-Legal-Levels.pdf (última visita: 16/4/2014).

[254] Ejemplo de sistema de identidad federado lo tenemos en RedIRIS es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Está financiada por el Ministerio de Economía y Competitividad, e incluida en su mapa de Instalaciones Científico-Técnicas Singulares (ICTS). Se hace cargo de su gestión la entidad pública empresarial Red.es, del Ministerio de Industria, Energía y Turismo. RedIRIS cuenta con más de 450 instituciones afiliadas, principalmente universidades y centros públicos de investigación, que llegan a formar parte de esta comunidad mediante la firma de un acuerdo de afiliación.
Disponible en: http://www.rediris.es/rediris/ (última visita: 11/4/2014).

dinero solicitado y, en algunos casos, obtener el saldo de la cuenta a fin de que el banco B lo pueda imprimir en el recibo de la transacción)[255].

De esta forma, lo que se está haciendo es decirle a los diferentes poseedores de los servicios o unidades de negocio internos es que: "este cliente es quien dice ser y, además, os lo aseguro. Podéis dejarle utilizar el servicio correspondiente". Ante esto, todos los participantes deben convenir una serie de reglas y protocolos para comunicarse y además fijar ciertos niveles de seguridad en las comunicaciones, privacidad de los datos del cliente y cumplimiento de las normativas legales correspondientes.

En las transacciones en línea, comúnmente la identificación y la expedición de los credenciales los ha efectuado la misma parte que tiene también la intención de exigir el credencial. Por ejemplo, una empresa identificará a un empleado y le asignará un nombre de usuario y una contraseña que le permita acceder a la red de la empresa. En tal caso, ésta actúa tanto como proveedor de la identidad (ya que ha identificado a la persona como su empleado y le ha expedido una credencial de identidad) y como parte receptora (puesto que también acepta y se sirve de esa credencial para autorizar el acceso a su red).

En un sistema de identidad "federado", las funciones del proveedor de la identidad y de la parte receptora no cumplen necesariamente la misma entidad. Por el contrario, múltiples partes receptoras, no relacionadas entre sí, pueden aceptar las credenciales de identidad que expida cualquiera de los diversos proveedores de identidad independientes. De acuerdo con este modelo, una única credencial de identidad puede ser aceptada por numerosas organizaciones que no hayan tenido participación directa en la expedición original de la credencial[256].

---

[255] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 3.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

[256] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 3.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

Si todos tuviéramos una única identidad; es decir, una única serie de datos asociados a su persona y que le definen ante diferentes instancias, como por ejemplo, nombre, apellidos, NIF, teléfono, correo electrónico, etc. El sistema de identidad federada se podría instaurar sin problemas. El problema es que no solo tenemos una identidad electrónica, sino que tenemos decenas de ellas: una en la empresa para la que trabajamos, otra en nuestra compañía de telefonía móvil, otra en nuestro banco, otra asociada a nuestra tarjeta de crédito, etc.

Hoy en día, todos tenemos múltiples identidades independientes en Internet. Las empresas, al igual que los consumidores, en sitios como Amazon, eBay, Facebook, etc. interactúan con diferentes identificadores para la autenticación de los servicios, que prestan sin que haya una conexión electrónica entre estas diferentes identidades.

Por ello, se hace indispensable algún tipo de procedimiento automatizado, algo que posibilite a los distintos sistemas de gestión, de la identidad de los participantes, negociar automáticamente, basándose en sus capacidades, como se intercambiarán ciertos datos de identidad de los usuarios (obviamente no el identificador de usuario y la contraseña), garantizando en el proceso la seguridad, privacidad de los datos y el cumplimiento de la ley[257]. Esto es exactamente lo que permite la federación de identidades.

En este sentido, la identidad federada surge en la ausencia de un sistema formal, coherente, transparente, eficiente y auditable de registro, que utiliza la criptografía estándar PKI y que anime a las organizaciones a su utilización a gran escala. Es importante el surgimiento de registros, capaces de hacer frente a un mayor volumen de transacciones, para que puedan devengar los muchos beneficios que esta tecnología puede ofrecer. La vulnerabilidad puede atribuirse al anonimato, es decir, a la falta de interoperabilidad que desalienta la realización intercambios de información confidencial mediante el Internet. La forma de eliminar este anonimato es a través del uso de

[257] SMEDINGHOFF, T. J.: "Solving the legal challenges of trustworthy on line identity", *Computer Law & Security Review*, octubre, 2012, vol. 28, núm.5, págs. 532-541.

registros y reclamar así una identidad digital. Un pequeño esfuerzo que parte de cada individuo[258].

Ante esta situación, el desafío al que enfrenta este movimiento mundial, es el establecimiento de un enfoque uniforme y confiable, para emisión y gestión de la identidad electrónica de los individuos, credenciales y derechos de uso. El beneficio para un usuario final es importante: permitirle el acceso a numerosas aplicaciones y servicios proporcionado a través de dominios y organizaciones mediante el uso de una misma credencial. De esta manera, los usuarios y los proveedores de servicios pueden depender de una sola identidad, para administrar la identidad de credenciales y en línea de forma segura[259].

3.1.2. Gestión de la identidad electrónica

La gestión de la identidad electrónica es una cuestión fundamental, para la mayoría de las transacciones de comercio electrónico y otras actividades en línea. Tengamos en cuenta que, desde una perspectiva jurídica, la identidad de un individuo es la base sobre la que se construyen los derechos y obligaciones de las personas; pues, en una relación entre dos o más sujetos, por ejemplo, en un contrato, o en cualquier

[258] MCKENNA, P.: "The probative value of digital certificates: Information Assurance is critical to e-Identity Assurance", *Digital evidence and electronic signature law review*, octubre, 2004, núm.1 , págs.55-60.

[259] El gobierno estonio ha aprobado la emisión de tarjetas de identificación inteligentes. Con ellas, los e-estonios (que no tienen que tener la nacionalidad de este país de la Unión Europea ni siquiera la residencia física en él), accederán a multitud de servicios online así como a la firma digital. Resulta especialmente interesante dos de sus características: 1) su obtención es voluntaria y abierta a todas las personas del mundo (no sólo de la Unión Europea); 2) No tiene en cuenta la residencia física ni la nacionalidad, puesto que la sociedad digital se mueve en otros parámetros y lo que en realidad se ofrece, por el Gobierno estonio, es la estructura digital a la que se puede acceder desde cualquier parte del mundo y los servicios que su utilización proporciona De esta forma, "puede parecer atrevido, desde postulados propios de un Segundo entorno (sociedad industrial), pero desde el tercer entorno (espacio virtual), en el que las relaciones aparecen mediadas tecnológicamente, la residencia digital pudiera ser un criterio a tener en cuenta" (DIAGO DIAGO, Mª.P.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario LA LEY*, núm. 8432, 2014, pág. 2). El servicio está dirigido, principalmente, a aquellos que ya tienen vínculos con Estonia, ya sea a través de negocios, estudios o por turismo. Se trata de plataforma que proporciona y utiliza servicios digitales en todo el mundo. Con ello, se espera que el e-residente atraiga a nuevos clientes a los servicios digitales de Estonia. (CUTHBERTSON, A., "Estonia First Country to Offer E-Residency Digital", *International Business Times* – Disponible en: http://www.ibtimes.co.uk/estonia-first-country-offer-e-residency-digital-citizenship-1468766 (última visita: 12/12/2014).
El texto completo de la Ley puede consultarse en: https://www.riigiteataja.ee/akt/129102014005 (última visita: 12/12/2014).

transacción con efectos jurídicos, se requiere una identificación de las personas que participan en ella como paso previo a su celebración.

En el mundo real la identidad y la identificación de las personas son materias de derecho sustantivo y del derecho procesal. La identificación de las personas que intervienen en la transacción es un elemento esencial del acto jurídico que se va a realizar, ya que el error sobre la identidad de la persona puede acarrear la nulidad del acto, al constituir un vicio del consentimiento que invalida la relación jurídica. La identificación hace referencia tanto a los datos de identidad de una persona como al acto y procedimiento de comprobación y acreditación de la identidad. De esta forma, podemos decir que las Leyes son las que definen los instrumentos y procedimientos que serán considerados válidos para la identificación de una persona[260].

En el mundo en línea, pasa lo mismo, aunque las partes se encuentran ausentes. Así pues, los participantes en la transacción electrónica tienen que confiar en un proceso de identificación que se va realizar de una persona con la expedición del correspondiente credencial. Ante esta situación surge una necesidad: la gestión de la identidad electrónica que podemos definirla como la definición, designación y administración de atributos de identidad[261].

Por un lado, debemos tener en cuenta que la gestión de la identidad no es un concepto nuevo, a pesar de que el término parece ser de origen reciente. Todos los gobiernos y las entidades privadas han empleado desde hace tiempo tarjetas de identificación u otros documentos para identificar a las personas como medios para autenticar la identidad; por otro, no se refiere a un solo sistema específico, sino más bien a una categoría de soluciones interrelacionadas, utilizadas para administrar la autenticación de usuarios, derechos de acceso y restricciones, perfiles de cuenta, contraseñas y otros atributos.

---

[260] CENTRO LATINOAMERICANO DE ADMINISTRACIÓN Y DESARROLLO (CLAD): "Marco para la identificación electrónica social iberoamericana", *Aprobado por la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado*, Asunción, 30 junio – 1 julio, 2011, pág. 12.

[261] GOVERNMENT UNIT, DG INFORMATION SOCIETY AND MEDIA, EUROPEAN COMMISSION: *The Modinis IDM Study Team: Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management*, Version 2.01, 23 de noviembre de 2005, pág. 11.

La idea de la que partimos es que la gestión de la identidad electrónica que se aplica a las personas es una preocupación primordial para empresas, gobiernos e individuos de todo mundo. Todos tratan de establecer una colaboración que implique tanto a los proveedores de identidad y otros proveedores de servicios.

Se trata de buscar la verificación de la identidad de partes alejadas en la transacción que tratan, por ejemplo, de acceder a una base de datos en línea que contienen información confidencial, para realizar una transferencia en línea de fondos con cargo a una cuenta, o que han firmado un contrato electrónico, quien ha enviado un correo electrónico o quien ha autorizado a distancia el despacho de un producto o enviado un correo electrónico[262].

La gestión de la identidad puede realizarse de diferentes formas, constituyéndose diversos tipos de sistemas de gestión de la identidad, que lo trataremos adelante, que pueden ser, desde el uso del nombre de usuario y contraseña, que a veces podemos considerarlo engorroso por tener que rellenar formularios, cuando realmente lo que pretendemos es acceder rápidamente a la aplicación o a la realización de la transacción; hasta la gestión de identidades digitales, dando lugar al desarrollo de sistemas de gestión de identidades, que pueden permitir el paso de las identidades electrónicas a través de fronteras mediante colaboración de entidades. En esta colaboración, dentro y a través de los sistemas de información, de múltiples organizaciones, se vienen a plantear cuestiones tecnológicas, organizativas y jurídicas[263]:

a) En términos de tecnología, los colaboradores tienen que decidir sobre una arquitectura que soporta la comunicación de la identificación datos.

b) A nivel organizativo, los colaboradores necesitan integrar algunos de sus procesos de negocio con el fin de lograr la interoperabilidad.

---

[262] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 6.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

[263] TOBIAS, M; THOMAS, O.: "Risk, responsibility and compliance in circles of Trust", *Computer Law & Security Review*, 2007, vol. 23, núm. 3, págs. 342 – 351.

c) Desde un punto de vista jurídico, la cooperación sobre la gestión de la identidad es un reto en términos del marco necesario contractual, la asignación de responsabilidades y, por último pero no menos importante, la protección de la información personal.

En este contexto, apreciamos que, los participantes en una transacción de bajo riesgo realizada en línea, tienden a confiar en que están tratando con una persona o entidad concreta, a medida que aumenta la confidencialidad o que incrementa el valor de la transacción, también crece la importancia de garantizar la disponibilidad y fiabilidad de la información exacta, acerca de la identidad de la parte que se encuentra a distancia, a fin de tomar una decisión, que se va a fundar en la confianza.

La situación que se plantea es la de crear un sistema de credenciales de identidad en línea, seguro, fiable y fehaciente y que pueda utilizar a distancia, en el marco de sistemas y entidades diferentes.

Observemos que la gestión de identidades, esencialmente, podría concretarse en dos procesos fundamentales[264]:

a) Identificación: el proceso necesario para la verificación de ciertos atributos de identidad de una persona y la emisión de una credencial de identidad, ligadas a esa persona para reflejar esos atributos.

b) Autenticación: los procesos necesarios para verificar a la persona que representa el credencial y, además, dice ser la persona descrita por esos atributos previamente verificados, de hecho, respecto a esa persona.

[264] PRICE, G: "The benefits and drawbacks of using electronic identities", *Information Security Technical Report,* mayo, 2008, vol. 13, núm.2, págs. 95 – 103.

El proceso de identificación está diseñado para responder a la pregunta "¿quién es usted?", tratando de asociar uno o más atributos, por ejemplo, un nombre, una dirección, la altura, la fecha de nacimiento, el número de la seguridad social, el empleador, un título, una matrícula, un número de socio, el cargo que ocupa en la empresa, etc. con una persona con el fin de identificar y definir a ese individuo, con un nivel suficiente de seguridad para la finalidad prevista[265].

Es decir, se trata de obtener una prueba de identidad, o mejor dicho, de probar la validez de una identidad, mediante el examen de los datos electrónicos generados, que a su vez son una colección de datos personales de un individuo que pretende ser identificado. Este proceso de identificación se lleva a cabo mediante un proceso de[266]:

a) Validez, a través de las pruebas que corroboran de manera suficiente la identidad de la persona; y,

b) Verificación, el usuario que solicita usar la identidad tiene derecho a asociarse con esa identidad.

Al final del proceso de identificación, la información acerca de la identidad del sujeto se representa típicamente por los datos proporcionados al proveedor de identidad, posteriormente éste los proporcionará a terceros, refiriéndose a estos como una identidad de credenciales[267].

Cuando hablamos de credencial nos referimos a los datos verificados relativos a uno o más atributos de identidad de una persona específica. En el mundo físico credenciales de identidad incluyen los Documentos Nacionales de Identidad, las licencias de conducir, pasaportes, tarjetas de identificación, etc. En el mundo virtual el credencial de identidad, como hemos mencionado antes, podría ser desde un nombre de

[265] SMEDINGHOFF, T. J.: "Solving the legal challenges of trustworthy online identity", *Computer Law & Security Review*, Vol. 28, octubre, 2012, pág. 532 – 541.
[266] PRICE, G: "The benefits and drawbacks of using electronic identities", *Information Security Technical Report*, mayo, 2008, vol. 13, núm.2, págs. 95 – 103.
[267] De esta forma, en todos los contratos de datos de prestación de servicios de certificación, tanto de persona física como de persona jurídica, podemos observar que la persona física solicitante del certificado declara que todos los datos, anteriores referentes a su identidad, son ciertos y veraces y en los Registros públicos competentes, que a la fecha de solicitud, tienen las facultades idóneas y suficientes, según se acredita, para solicitar un certificado electrónico de firma.

usuario o un certificado criptográfico digital que puede ser almacenado en un ordenador, en un teléfono móvil, en una tarjeta inteligente, tarjeta de cajero automático, una unidad flash o un dispositivo similar, etc.

Sí una persona presenta una credencial de identidad, por ejemplo, mediante la presentación de un pasaporte en un aeropuerto o introduciendo un nombre de usuario en una red corporativa, y trata de ejercer un derecho o un privilegio concedido a la persona descrita por ese credencial, por ejemplo, a bordo de un avión o para acceder a la red corporativa o una base de datos sensibles, se hace necesario un proceso de autenticación, que realizará el usuario que confía, para determinar si la persona que presenta la credencial es la persona descrita por esta credencial[268].

En otras palabras, cuando alguien dice ser la persona identificada por una credencial de identidad, se pasa a un proceso de autenticación[269], que está diseñado para responder a la pregunta "de acuerdo, ¿cómo se puede demostrar?". Es un evento de transacciones específicas, que implica la asociación de una persona con una credencial de identidad, para verificar que la persona, que trata de participar en la transacción, es realmente la que se ha identificado y autorizado para la transacción previamente[270].

Ante esto, no tardamos en darnos cuenta del problema: la gestión de la identidad que se ha venido usando, en entornos fuera de línea, han sido: los pasaportes, carnés de conducir, los documentos nacionales de identificación, etc.; es decir, documentos que componen sistemas de gestión de identidades de carácter nacional. Se tratan de credenciales expedidos por una autoridad nacional pública cuya identidad ha sido confirmada de modo que posteriormente puede ser demostrada dentro de un sistema propio, o lo que es lo mismo, dentro del propio sistema nacional.

---

[268] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 7.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

[269] MCKENNA, P.: "The probative value of digital certificates: information assurance is critical to e-identity assurance", *2008*, octubre, 2004, num. 1, págs. 55 – 60.

[270] SMEDINGHOFF, T. J.: "solving the legal challenges of trustworthy online identity", *Computer Law & Security Review*, Vol. 28, octubre, 2012, pág. 532 – 541.

No obstante, si observamos la identidad gestionada por un Estado dentro de su propio sistema nacional, casi en exclusividad, podemos examinar tres niveles de leyes o normas que parecen regir la gestión de identidades. La comprensión de estos tres niveles proporciona una mejor base para el análisis de las cuestiones jurídicas y la consideración de las posibles soluciones. Los tres niveles se pueden resumir de la siguiente manera[271]:

a) Nivel 1: Se trata de leyes y reglamentos de derecho público, adoptadas por los gobiernos, que se promulgan y aplican a nivel nacional. Estas leyes no son problemas específicos de identidad. No obstante, las leyes se aplican a la identidad nacional y su aplicación transfronteriza plantea incertidumbres siendo uno de los problemas esenciales a los que se enfrentan los sistemas de identidad.

b) Nivel 2: la ley de identidad específica o marcos voluntarios, que puede incluir normas de derecho público o de derecho privado según lo acordado por las partes en el contrato. Actualmente se están elaborando las normas que se rigen en este nivel, por ejemplo, en la UE, donde puede incluirse el Reglamento identificación electrónica.

c) Nivel 3: normas de funcionamiento del sistema de la identidad individual Este se sitúa en el ámbito del derecho privado, por lo general se trata de normas basadas en contratos desarrollados por y diseñados para un sistema de identidad específico con el fin de regular el funcionamiento de dicho sistema, un ejemplo es el empleado por entidades como VISA.

[271] ABA IDENTITY MANAGEMENT LEGAL TASK FORCE: M*eeting Report*, 10 – 11 diciembre, 2012.
Disponible en: http://meetings.abanet.org/webupload/commupload/CL320041/relatedresources/ABA-IdM-London-Meeting-Summary.pdf (última visita: 17/4/2014).

3.1.2.1. La emisión de credenciales para la gestión de la identidad electrónica

Cuando hablamos de credenciales[272] del mundo físico nos estamos refiriendo a documentos que, en rigor, son públicos y, a su vez, acreditan la auténtica personalidad de su titular, constituyendo el justificante completo de la identidad de la persona, siendo imprescindible para justificar por sí mismo quien es su titular. En el mundo en línea, en relación con el régimen de la equivalencia funcional de los elementos que legitiman al titular de la firma electrónica, que pretende identificarse en la transacción, y observando las directrices proporcionadas por las leyes, para su eficacia práctica y material, se trata de elementos que están en control exclusivo[273] del firmante; o sea, bajo un esquema igual que en el mundo físico, pues resulta necesario probar que está bajo posesión del firmante: en el caso de la firma digital, hablamos de la clave pública permitiendo identificar de manera segura a aquél; en el caso de las firmas electrónicas simples, hablamos de la necesidad de probar la identificación, haciéndose responsable de los datos aportados al rellenar un formulario, en el que en muchos casos te piden un número de DNI, una cuenta de correo electrónico, etc.

La emisión de credenciales, en los sistemas de gestión de identidades electrónicas, se delega a un proveedor de identidad con el objetivo de cubrir el marco jurídico y organizativo que se tiene que abarcar. Si tenemos en cuenta el trato tecnológico preferente que se ha dado a las leyes de firma electrónica en algunos Estados, en pro de la administración electrónica, han cedido competencias de emisión a proveedores de servicios públicos de certificación dotándoles de una posición preferente.

Por otro lado, en este proceso de identificación, los proveedores de servicios de certificación privados necesitan confiar en el proveedor de identidad, que normalmente será nacional, con respecto a la autenticación de los usuarios nacionales. Esto requiere diligencia no sólo respecto a la autenticación en sí, sino también con respecto a todas las

[272] REINIGER, R. T.: "The proposed international e-identity assurance standard for electronic notarization", *Digital evidence and electronic signature law review*, octubre, 2008, núm. 5, págs. 78 – 80.
[273] ALBA, M.: "Necesidad para el comercio internacional de una regulación armonizada sobre documentos electrónicos negociables", CNUDMI, 28 de enero, 2011.
Disponible en: http://www.uncitral.org/pdf/english/colloquia/EC/MAlba_Paper_Negotiable_Docs.pdf (última visita: 31/3/2014).

fases anteriores. Por lo tanto, uno de los problemas más evidentes a tratar: es la fuerza y la calidad de los procedimientos de pre-registro y autenticación realizadas por proveedores de identidad que, centrándose en aspectos nacionales, dejan al margen cualquier aspecto de reconocimiento internacional[274].

Esto se ve en la propia designación y administración de atributos de identidad, pues, teniendo presente que a la luz de la identidad nace la determinación de la nacionalidad, que viene establecida por el DNI (documento público obligatorio a partir de determinada edad que acredita la identidad, la nacionalidad y demás datos en él contenidos de su titular). Esta nacionalidad debe determinarse con arreglo al Derecho del país, cuya nacionalidad dice ostentar el sujeto. Según el Derecho Internacional Público, cada Estado dispone de competencia exclusiva para determinar que personas ostentan su nacionalidad. Asimismo, el TJUE ha indicado que la atribución o pérdida de la nacionalidad de un ciudadano de un Estado miembro es competencia exclusiva de dicho Estado miembro, puesto que ello afectaría a un ciudadano de la UE; el ejercicio de esa competencia puede ser sometido a un control jurisdiccional a realizar con arreglo al Derecho de la UE[275].

De esta forma, observamos cómo en la mayoría de las leyes sobre firma electrónica[276] establecen un marco normativo, que de manera transversal afecta a todo el ordenamiento jurídico, civil, mercantil, administrativo, etc. Bien de manera expresa o bien a través de cláusulas de salvaguarda que permiten la intervención estatal. Todo ello se manifiesta con mayor claridad se manifiesta en el propio DNI electrónico, que se presenta como un elemento esencial dentro del sistema y que no permite a los sujetos usarlo fuera de él.

[274] En este sentido, si entendemos la identidad como un conjunto de atributos referidos a la personalidad, que permiten la individualización de un sujeto en sociedad, debiendo resaltarse que es una condición cultural, social y espacial, es decir, rasgos que tienen en relación con un entorno político. La falta de identidad impide el acceso a la vida económica, social y política de un país. Por ello, la identidad se garantiza por los poderes públicos mediante la organización del registro civil, la existencia de la persona y las estadísticas vitales de la misma.

[275] CALVO CARAVACA, A. L. y CARRASCOSA GONZÁLEZ, J.: *Derecho Internacional Privado*, Granada, 2012, pág. 17 y ss.

[276] Puede verse, especialmente, España (Ley 59/2003 de 19 de diciembre, de firma electrónica), Italia (Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale") o Inglaterra (Electronic Communications Act (2000).

En este contexto, la situación que se nos presenta es que, en la mayoría de los casos, los ciudadanos de un Estado no pueden utilizar su identificación electrónica para autenticarse en otro país porque los sistemas nacionales de identificación electrónica en su territorio no son reconocidos en aquel. Dicha barrera electrónica excluye a los prestadores de servicios del pleno disfrute de los beneficios del propio mercado. Unos medios de identificación electrónica mutuamente reconocidos facilitarán la prestación transfronteriza de numerosos servicios en el mercado y permitirán, tanto a las personas físicas como jurídicas, actuar fuera de sus fronteras sin encontrar obstáculos en su interacción con las autoridades públicas.

El motivo es que cada organización tiene sus mecanismos de identificación electrónica propios y en muchos casos no son compartidos con otros departamentos o usuarios[277]. En un ámbito más cercano, reflexionemos sobre la problemática de la gestión de la identidad electrónica a nivel europeo con los Estados miembros de la Unión Europea[278], cada uno con su propia idiosincrasia y diferentes avances en materia de identificación electrónica y, por supuesto, con sus propias diferencias en sus sistemas jurídicos.

Por un lado, en Reino Unido, se utilizan de forma masiva técnicas de autenticación menos seguras y livianas como "nombre usuario y clave" o identificación por e-mail, sin desarrollar de manera plena la identificación basada en certificados electrónicos reconocidos. A esto hay que añadir, el intento de Reino Unido de establecer un documento de identificación personal a través de la *The Identity Cards Act* de 2006[279]. Esta Ley estuvo en vigor hasta 2010, fecha en la que fue derogada, por las fuertes críticas y reticencias de los ciudadanos, lo que llevó a establecer la cancelación de la tarjeta de identidad nacional, así como, todos los datos personales emitidos con una tarjeta de identidad que fueron registrados en el Registro Nacional de Identidad, lo que incluía fotografías y datos biométricos, huellas dactilares, etc.[280]

---

[277] ÁLVAREZ RODRÍGUEZ, M.: "El DNIe español como puerta de entrada a servicios de Administración electrónica en Europa: Proyecto STORK".
Disponible en: http://administracionelectronica.gob.es/ctt/resources/1a7be7bd-1492-46e3-a6e2-88772fea046f?idIniciativa=213&idElemento=320 (última visita: 31/3/2014).

[278] STORK:
Disponible en: https://www.eid-stork.eu/ (última visita: 31/3/2014).

[279] The Identity Cards Act (2006).
Disponible en: http://www.legislation.gov.uk/ukpga/2006/15/contents (última visita: 31/3/2014).

[280] Derogación de la Identity Cards Act.

Por otro lado, la mayoría de los países europeos[281] ya empiezan a implantar certificados digitales basados en soluciones de PKI (el 75% de los países europeos ya tienen desplegados soluciones de PKI más o menos extendidas según el Informe de IDABC de la Comisión Europea sobre Diferencias y Similitudes en materia de e-ID[282]). Por último, otros países están a la vanguardia de la identificación electrónica, al emitir tarjetas nacionales criptográficas, que incluyen la firma reconocida y la autenticación más fuerte, basada en certificados digitales sobre un soporte de dispositivo seguro de creación de firma con chip; entre ellos, como hemos detallado: España con nuestro DNI electrónico, Alemania, Italia, Austria, Bélgica, Finlandia, Estonia y Suecia.

Fuera de la Unión Europea, Australia[283] está debatiendo la incorporación de tarjetas de identificación, el proyecto de ley ha sido dos veces rechazado por el Senado solicitando una ley adicional que proporcione garantías y asegure que esta tarjeta no se convierta en un documento nacional de identidad. Corea del Sur y Taiwán también han encontrado oposición al establecimiento de tarjetas de identidad, deteniendo sus proyectos ante las protestas por el alto costo económico y los escándalos de robos de identidad y falsificación de las tarjetas de identificación[284]. Asimismo, en Estados Unidos[285], los planes de convertir la licencia de conducir en un sistema nacional de identificación, se ha encontrado con una férrea resistencia de los propios Estados de la Unión y organizaciones públicas[286].

Disponible en: https://www.gov.uk/identity-cards-and-new-identity-and-passport-service-suppliers (Disponible en: 26/3/2014).

[281] RÖSSLER, T.: "Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government", *Computer Law & Security Review*, 2008, vol. 24, núm. 5, págs. 447 – 453.

[282] IDABC: *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*.
Disponible en: http://ec.europa.eu/idabc/ (última visita: 21/4/2014) (Esta Web ha quedado sin actividad desde 2009 a favor de ISA: Interoperabily Solutions for European Public Administrations.
Disponible en: http://ec.europa.eu/isa/ (última visita: 21/4/2014).

[283] AUSTRALIAN PRIVACY FOUNDATION:
Disponible en: http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html (última visita: 31/4/2014);
ELECTRONIC FRONTIERS AUSTRALIA:
Disponible en: http://www.efa.org.au/Issues/Privacy/accesscard.html. (última visita: 31/3/2014).

[284] ELECTRONIC PRIVACY INFORMATION CENTER: *Real ID implementation review: few benefits, staggering costs. Analysis of the department of homeland security's national id program electronic privacy information center*, mayo, 2008.

[285] REAL ID Act of 2005, L. 109-13, 199, Stat. 302, aprobada el 11 de mayo de 2005.
Disponible en: http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/html/PLAW-109publ13.htm (última visita: 31/3/2014).

[286] Por ejemplo el Estado de Utah se opuso a la REAL ID Act mediante "Resolution Opposing REAL ID ACT 2007Gereral Session".

Así pues, a la hora de identificar al firmante, de forma que pueda crearse una firma electrónica válida y segura, nos encontramos ante un problema de verificación de la identidad, como requisito imprescindible para la viabilidad de las firmas electrónicas en un contexto internacional.

En este sentido, se puede observar cómo los Estados tratan de dar prioridad identificativa a las tarjetas de identificación, que están orientadas a atender las necesidades de sus ciudadanos y, con ello, a tratar de establecer medidas que definan una tecnología y un proceso de identificación determinado capaz de confirmar con seguridad la identidad de la persona en cuestión, tratando de obtener la confianza del ciudadano[287].

Igualmente, estas tarjetas de identificación[288] vienen a ofrecer una prueba de identidad, dentro de su propio sistema, en el que una autoridad nacional, creíble y reconocida, puede confirmar, que una persona física determinada es la que se identifica con un nombre, apellidos, fecha de nacimiento, dirección que se le atribuye, etc.[289].

Como hemos visto, son muchos los países que cuentan con sistemas de identidad nacional, utilizados para una gran variedad de propósitos, públicos o privados; otros países no cuentan con ellos, pero se debate sobre su incorporación. Entre los que se encuentran con sistemas de identidad están: España, Alemania, Italia, etc. También Estados Unidos, aunque, sus planes de convertir la licencia de conducir en un sistema de identificación se han ralentizado debido a la resistencia de muchos Estados y

---

Disponible en: http://le.utah.gov/~2007/bills/hbillenr/hr0002.htm (última visita: 31/3/2014).

[287] SOBEL, R.: "The Degradation of Political Identity under a National Identification System", *Boston University Journal of Science & Technology Law*, 2001.
Disponible en: http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume81/sobel.pdf (última visita: 31/3/2014).

[288] ÁLVAREZ RODRÍGUEZ, M.: *El DNIe español como puerta de entrada a servicios de Administración electrónica en Europa: Proyecto STORK*.
Disponible en: http://administracionelectronica.gob.es/ctt/resources/1a7be7bd-1492-46e3-a6e2-88772fea046f?idIniciativa=213&idElemento=320(última visita: 31/3/2014).

[289] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 7.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita 26/3/2014).

organizaciones públicas. Entre los que no cuentan están países como Australia, Reino Unido, Canadá, etc.[290].

En este contexto, en nuestra opinión, debe observarse la acción de identificar a las personas que quieren ser identificadas electrónicamente a través de datos personales, necesarios para ser reconocida, o por el acto de reconocer que la persona es la misma que se supone o que se busca, lo que nos da la identificación; y ésta, la identidad, como conjunto de rasgos propios de un individuo o de una colectividad que los caracteriza frente a los demás, con la coincidencia de que una persona tiene que ser ella misma y, por tanto, distinta a las demás. Estos datos vienen dados dentro del enfoque discriminatorio que se le suele dar a las leyes en base al reconocimiento de certificados del país de origen.

De esta forma, lo comentado anteriormente, nos permite llegar a la conclusión de que todo está adaptado al estado discriminatorio de las Leyes respecto a los certificados electrónicos que han sido emitidos por las entidades públicas de los Estados, bien en tarjetas inteligentes (e-DNI), o bien de cualquier otra manera, conforme a las leyes aprobadas que buscan preservar, antes que nada, la seguridad de sus ciudadanos, lo que lleva aparejada la discriminación de los certificados de origen emitidos, en terceros países por la propia intervención de las administraciones públicas. Y esto es así, porque el derecho es quien define qué instrumentos y procedimientos serán considerados válidos para la identificación de una persona. El Estado es el encargado de identificar a las personas, a partir de distintos procedimientos según la legislación del país de que se trate.

Centrándonos en España, donde la Ley 59/2003, de 19 de diciembre, sobre firma electrónica, partiendo de la Directiva comunitaria 1999/93/CE sobre firma electrónica de índole privatista y de protección del consumidor, se recogen diferentes modelos normativos que afectan al orden civil, mercantil, administrativo, a la seguridad pública y que presenta especialidades de aplicación exclusiva para la Administración General del

[290] SCHEERES, J.: "ID Cards Are de Rigueur Worldwide", *Wired News*, 25 de septiembre de 2001. Disponible en: http://www.wired.com/news/conºict/0,2100,47073,00.html (última visita: 31/3/2001).

Estado, mostrando intereses políticos internos de la Administración pública que se manifiesta con el establecimiento del DNI electrónico[291].

En el desarrollo del comercio electrónico intervienen entes privados y públicos. Sin embargo, su actuación no se desenvuelve en régimen de libre competencia ni bajo el ordenamiento jurídico privado. Esta afirmación es aplicable especialmente a la actividad certificadora en relación con la firma electrónica.

En España, el DNI electrónico es emitido por un prestador de servicios público, la Fábrica Nacional de Moneda y Timbre[292]. Este DNI incluye medios tecnológicos necesarios para firmar y verificar la firma de documentos electrónicos (uso de una infraestructura de clave pública), además, se puede utilizar para identificarse y firmar por medios electrónicos.

Este DNI puede tener un posible uso general, no solo administrativo sino también comercial. Aun cuando no se establece expresamente, pueden hallarse distintos argumentos a favor de esta interpretación amplia de la Ley 59/2003 de firma electrónica. En primer lugar, el DNI electrónico tiene plena eficacia para acreditación de la identidad, sin distinguir el ámbito administrativo o no, en el que producirán tales efectos; en segundo, se establece de forma expresa que todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia identificativa del DNI electrónico[293].

Ante esto, se puede comprender que, con la obligatoriedad de su obtención, su reducido coste y su obligatorio reconocimiento, a tenor de lo expresado anteriormente, se puede llegar a la conclusión de que esta firma electrónica establecida en el e-DNI será la única que utilicen las personas físicas, no sólo en el ámbito administrativo, sino

[291] COUTO CALVIÑO: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista de la Contratación Electrónica*, 2007, núm. 83, págs. 3 – 27.
[292] CERES – FNMT:
Disponible en: http://www.cert.fnmt.es/ (última visita: 31/3/2014).
[293] MARTINEZ NADAL, A.: *Cometarios a la ley 59/2003 de Firma Electrónica*, Madrid, 2009, pág. 278 y ss.

también en el comercial o en las relaciones jurídico-privadas, dándose a la postre una quiebra flagrante de la libre competencia[294].

Por otro lado, los certificados de empresas, también, son emitidos, casi en exclusividad por entidades de carácter público, entre las que destacan ANCERT[295] (Agencia Notarial de Certificación) y CAMERFIRMA[296] (Servicio de certificación digital de las cámaras de comercio, industria y navegación de España).

Ante esta situación, se da la existencia de un sistema de identificación gubernamental, produciéndose una identidad "oficial", que luego puede ser reproducida en procesos de identificación posteriores. El Estado hace uso de sus propios instrumentos, para el registro obligatorio y la identificación de cada uno de sus ciudadanos y cada una de las empresas, con el fin de establecer tal identidad. Se actualiza durante largos períodos de tiempo, no sólo en forma de tarjetas de identidad y pasaportes oficiales, sino también a través de inspecciones de registros[297]. Ambos procedimientos conducen al tratamiento de datos personales y, en última instancia, a la difusión del conocimiento entre los interlocutores sobre el titular de la tarjeta de identificación. Todo esto, hace que entes privados no puedan entrar en el mercado en igualdad de condiciones y que el reconocimiento internacional quede lejos, salvo acuerdo internacional.

3.2. Autenticación de la identidad electrónica

Como hemos dicho antes, la gestión de la identidad se lleva a cabo mediante dos procesos fundamentalmente: a) validez, los atributos de identidad que corresponden a una persona permiten expedir un credencial de identidad que refleje aquellos atributos;

[294] COUTO CALVIÑO, R.: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista de la Contratación electrónica*, , 2007, núm. 83, págs. 3 – 37.
[295] ANCERT:
Disponible en: http://www.notariado.org/liferay/web/cien/indice-unico-informatizado/ancert/la-apuesta-tecnologica-del-notariado (última visita: 31/3/2014).
[296] CAMENFIRMA:
Disponible en: http://www.camerfirma.com/ (última visita: 31/3/2014).
[297] FROOMKIN, A. M.: "Creating a viral federal privacy standard", *Boston College Law Review*, 2006, págs. 55 – 86.
Disponible en: http://law.tm/docs/virtial-privacy-standard.pdf (última visita: 31/3/2014).

b) verificación, a través de la cual una persona determinada que presenta el credencial y sostiene que es la persona previamente identificada.

La autenticación de la identidad[298] debemos relacionarla con el proceso de verificación de la afirmación que se hace relativa a la identidad o al atributo perteneciente a dicha identidad. Estos procesos se realizan a través de los llamados sistemas de gestión.

Para estos procesos de verificación, los ordenamientos jurídicos de algunos Estados, considerando la necesidad de que se cumplan una serie de requisitos en relación con la comunicación electrónica, se han decantado por dar preferencia a una determinada tecnología. La razón la encontramos en la equivalencia funcional; es decir, cuando la firma electrónica es funcionalmente equivalente a la firma tradicional[299].

Por esto, se observa que, en el estado actual del comercio electrónico y la firma electrónica, a la vista de la gran variedad de tecnologías reguladas, procedimientos o requisitos de forma, que son requeridos de un Estado a otro, para la autenticación, plantean grandes problemas, pues los términos que se recogen en las distintas leyes estatales no ostentan conceptos universalmente aceptados.

Mientras en el derecho anglosajón, la pertinencia de un documento como elemento de prueba se establece al vincularlo a una persona, lugar o cosa, de tal manera que firmar y autenticar suelen identificarse como sinónimos. De tal manera que la rúbrica puede ser todo nombre o símbolo utilizado por una persona con la intención de que se constituya como su firma, entendiéndose que toda la finalidad de las normas que prescriban que un documento concreto sea firmado por una persona concreta es confirmar la autenticidad del documento. Por otro lado, en los foros romanistas, se ha

[298] ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN (ISO): *Glossary of IT Security Terminology, SC 27 Standing Document 6*, 31 de marzo de 2002, pág. 5; define la autenticación de la identidad como: "la condición de garantía de la afirmación de identidad de una entidad".
Disponible en:
https://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf (última visita: 1/4/2014).
GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET (IETF): *Internet Security Glossary, RFC 2828, IETF Network Working Group*, mayo de 2000. Define la autenticación como "el proceso de verificación de una identidad afirmada por o para una entidad del sistema".
Disponible en: http://www.ietf.org/rfc/rfc2828.txt (última visita: 31/3/2014).
[299] DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009, pág.80 y ss.

adoptado la regla de la libertad de forma, para compromisos contractuales en asuntos de derecho privado. Suelen interpretar las normas probatorias de una forma más estricta. Así, el término autenticación se interpreta en el sentido de que la autenticidad de un documento ha sido verificada por una autoridad pública competente o un notario, siendo frecuente referirse a la noción de originalidad de los documentos.

Ante esto, deben considerarse todas las circunstancias relevantes en el momento que se realiza la firma; por ejemplo, el método que se utiliza para autenticar el documento electrónico, pues, este debe ser tan fiable como sea apropiado para los fines para los cuales se crea. No considerar esto podría suponer una seria debilidad del sistema de firma electrónica que se establezca en el foro.

Si decimos que una firma electrónica es cualquier medio de autenticación electrónica de la identidad de un sujeto y de la intención de éste, indicando aprobación y asociación con un registro electrónico; o sea, podemos decir que la autenticación electrónica es un término utilizado para referirse a diversas técnicas destinadas a reproducir en un entorno electrónico las funciones señaladas como característica de las firmas manuscritas[300].

Ante esta situación, cabría decir que la autenticación es firmar, para establecer como verdadero o asociarse asimismo con un documento[301], lo que nos permite llegar a la afirmación, con la que empezamos este capítulo: autenticación es el proceso de verificación de una identidad.

Normalmente, es el vendedor quien se autentica ante el comprador, aunque también puede ocurrir que el comprador se autentique ante el vendedor o servicio de pago[302]. En cualquier caso, este proceso es muy importante; pues, el cliente necesita estar seguro de que dialoga con quien cree hacerlo, para no proporcionar, por ejemplo, sus datos bancarios o cualquier dato de carácter personal, que pudiera ser usado de

[300] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 15.
[301] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, págs.25 y ss.
[302] MATA Y MARTÍN, R. M.; JAVATO MARTÍN, A. Mª.: L*os medios electrónicos de pago: problemas jurídicos*, Granada, 2007, págs. 8 y ss.

modo fraudulento. Por otro lado, el comerciante requiere verificar la identidad del comprador para evitar una actitud fraudulenta o el repudio del mensaje, la compra, etc.

Dicho con otras palabras, se trata de establecer la acreditación por medios electrónicos de la identidad de una persona o ente con respecto al contenido de la voluntad expresada en sus operaciones, transacciones y documentos, y de la integridad y autoría de estos últimos.

Por ello, podemos decir que la firma electrónica se encuentra asociada al uso de la función identificativa y la función autenticadora, estando ambas funciones asociadas en la firma electrónica de forma ineludible, de tal manera que el uso de una implica la utilización de la otra. Ambas van aparejas en la firma electrónica, en el sentido de que el uso de la misma siempre se vincula, de forma esencial, a la declaración de voluntad[303]; pues, en una relación entre dos o más personas, con efectos jurídicos, es necesario acreditar la identidad de las partes que intervienen en ella.

Un contrato, una demanda, una adquisición, una venta, etc.; es decir, toda operación con efectos jurídicos requiere la identificación de las personas que participan de ella, como paso previo a su celebración. La identificación de las personas es un elemento esencial de los actos jurídicos, ya que el error sobre la identidad de la persona acarrea la nulidad del acto, al constituir un vicio del consentimiento, que invalida la relación jurídica. Esto se lleva a cabo mediante los llamados sistemas de gestión de la identidad.

3.2.1. Los sistemas de gestión de la identidad como medio de autenticación

Los sistemas de gestión de la identidad son infraestructuras técnicas y organizativas para la definición, gestión y administración de las identidades electrónicas; es decir, un sistema integrado de políticas o procesos organizados que pretenden facilitar y controlar el acceso a los sistemas de información[304].

[303] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica,* Madrid, 2009, pág. 85 y ss.
[304] PRICE, G.: "The benefits and drawbacks of using electronic identities", *Information Security Technical Report*, mayo, 2008, Vol. 13, núm. 2, mayo, 2008, Pags.95-103.

Estos sistemas son utilizados por todos los países del mundo de distintas maneras, hasta tal punto que los sistemas, y con ellos las tecnologías utilizadas, varían enormemente entre unos y otros.

La gestión de la identidad electrónica va a depender, en gran medida, de las características del servicio al que se accede, ya que unos requieren la aportación de un dato, que sólo conoce el usuario y el suministrador del servicio (por ejemplo, una casilla de la declaración del IRPF); otros, requieren la inscripción previa en un registro del propio servicio, que facilita unas claves o contraseñas para acceder y utilizarlo (el método de usuario/contraseña); también, se puede acceder a dichos servicios electrónicos mediante DNI electrónico, que acredita y garantiza la identidad, en la red, de una persona; igualmente se requieren certificados electrónicos de empresa, para el acceso seguro a los servicios (tarjetas inteligentes), además, verificación de la identidad de una persona en base a características fisiológicas o de comportamiento; así como huellas dactilares, escaneos de retina; la biometría de la geometría de las manos o las "impresiones palmares"; o tecnología de reconocimiento de voz (datos biométricos), etc.

En definitiva, decimos que la autenticación de la información puede consistir en algo que una persona sabe (contraseña, PIN), posee (tarjeta inteligente, e-DNI, pasaporte), o es (datos biométricos). Se trata de factores basados en el conocimiento y en la posesión que requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo. De esta forma, cuando una persona presenta un credencial, la parte receptora recurre a un proceso de autenticación para determinar si esa persona es quien afirma ser. La autenticación tiene por objeto responder a la pregunta: "¿cómo puede probar quien dice usted que es?"[305].

La autenticación de la identificación electrónica implica la presentación de la información de manera que se confirme la asociación entre una persona y un identificador, lo que entraña la necesidad, en algunas legislaciones como puede verse;

[305] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 8.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita: 26/3/2014).

por ejemplo, en el Reglamento (UE) Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, que atiende a distintos niveles de seguridad, lo que a su vez supone cumplir determinados requisitos técnicos. Esto nos lleva al riesgo de que la parte receptora tenga la capacidad de autenticarla; es decir, de vincular los atributos de identidad declarados por el sujeto de manera correcta. De esta forma, podemos decir que la autenticación incluye tanto el riesgo de que un sujeto legítimo no pueda ser adecuadamente objeto de autenticación y el riesgo de que el proceso de autenticación indique incorrectamente que un impostor es el sujeto legítimo[306].

El acceso a la información de autenticación permite asumir la identidad verificada. Sin embargo, el conocimiento o posesión de la información objeto de autenticación no implica automáticamente que esté en conocimiento o en posesión de la persona a la que le pertenece por derecho, algo que sucede con cierta frecuencia en la práctica empresarial.

Las transacciones de comercio electrónico se realizan a distancia y la invocación de la buena fe, como principio básico, es importante en cualquier caso. En la conducta negocial, la regla de la buena fe, nos permite aseverar que la autenticación es firmar, para establecer como verdadero o asociarse a sí mismo con un documento y pueda referirse a la verificación de la identidad.

En consecuencia, se trata ha de proporcionar un marco jurídico para el reconocimiento transfronterizo y la interoperabilidad de la autenticación de la identidad electrónica; lo que supone tener como objetivo el establecimiento de unas medidas legales, que nos llevan a garantizar el reconocimiento mutuo de la identificación y de la autenticación de la identidad electrónica.

Así se ha concebido en Estados Unidos en la *E-Sign*, dentro de un marco tecnológicamente neutral, que considera que las firmas electrónicas son el equivalente funcional de las firmas manuscritas siempre que la tecnología empleada tenga la

[306] MASON, S.: "Validating identity for the electronic environment", *Computer Law & Security Review*, mayo, 2004, vol.20, núm. 3,vol. 3, págs.164-170.

finalidad de desempeñar determinadas funciones específicas y cumpla, además, determinados requisitos de fiabilidad[307]. Estas funciones son: identificar al firmante e indicar la intención del firmante respecto de la información firmada.

También, en Singapur, una firma electrónica se declara segura si cumple los requisitos del artículo 18 de la *Electronic Transaction Act*:

a) Es única la persona que la utiliza,

b) Es capaz de identificar a la persona,

c) Está bajo control exclusivo de la persona que la utiliza.

De esta manera, se especifica un procedimiento de seguridad, o un "procedimiento de seguridad comercial razonable", acordado por las partes involucradas, conforme al Artículo 17, a través del cual se puede verificar si el documento electrónico no ha sido alterado en el tiempo.

Igualmente, apreciamos que estas leyes, que son neutrales tecnológicamente, prestan una gran atención a la identidad y a la autenticación, como elementos esenciales para garantizar la seguridad de los datos. Se trata de reconocer la necesidad de promover la confianza en la integridad y la confiabilidad del comercio electrónico, minimizar el fraude, así como, eliminar toda posible falsificación y alteración de los registros económicos, mediante el establecimiento de reglas uniformes que regulen la integridad y autenticación de los registros electrónicos[308].

Las Leyes mencionadas tienen en cuenta el riesgo que supone la autenticación, en el sentido de que, la identificación no tiene utilidad a menos que la parte receptora tenga la capacidad de autenticarla; es decir, capacidad de vincular los atributos de identidad declarados con el sujeto correcto. El riesgo en la autenticación incluye, tanto el riesgo de que un sujeto legítimo no pueda ser adecuadamente objeto de autenticación como el

[307] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.83.
[308] TER HAH LENG: "E – Commerce: new law on e- commerce: Singapore", *Review Computer Law & Sevurity Report*, 1999, núm. 1, vol. 15, pág. 9.

riesgo de que el proceso de autenticación indique incorrectamente que un impostor es el sujeto legítimo.

Ante este panorama, ambas leyes reconocen todo tipo de firmas, siendo las que cumplan con los criterios establecidos, las que se consideran automáticamente como firmas electrónicas fiables a todos los efectos.

En otro extremo, tenemos sistemas, como el europeo, que en sus de diferentes normas jurídicas establecen disposiciones tecnológicas, especificando normas técnicas que deben seguirse, olvidando el principio de neutralidad tecnológica. Se trata de normas, que además, no definen con exactitud los derechos, obligaciones y responsabilidades de los participantes en el sistema de gestión de la identidad, sin que tampoco aclaren los riesgos legales, que las partes asumen al participar en el propio sistema (por ejemplo, las garantías, la responsabilidad por las pérdidas, las medidas de daños y riesgos para los datos personales). Ante esto, se observa como las leyes se han construido sobre el término seguridad, entendiendo la seguridad en el sentido más estricto de la palabra.

3.2.1.1. Principales sistemas de gestión de identidad

3.2.1.1.1. Contraseñas y métodos híbridos

En el comercio electrónico, para controlar el acceso a la información o servicios y para firmar comunicaciones electrónicas, se utilizan contraseñas y códigos. Estos métodos son los más utilizados a efecto de control del acceso y verificación de la identidad en una gran diversidad de operaciones, incluidas casi todas las bancarias por Internet y la retirada de efectivo en cajeros automáticos, así como las compras con tarjeta de crédito.

Se debe reconocer que es posible utilizar muchas tecnologías para autenticar una operación. En una operación determinada pueden emplearse varias de ellas o diversas versiones de la misma. Por ejemplo, la dinámica de la firma efectos de autenticación puede conjugarse con criptografía para ratificar la integridad del mensaje.

Opcionalmente, puede transmitirse contraseñas por Internet mediante criptografía para protegerlas, conjuntamente con la utilización de sistemas biométricos para crear una firma digital (criptografía asimétrica), que al recibirse genera un justificante de autenticación del protocolo de Kerberos[309] (criptografía simétrica).

Al elaborar marcos jurídicos para reglamentar estas tecnologías, se debe prestar atención a las de carácter múltiple. Los marcos jurídicos normativos de los sistemas de autenticación electrónica deberán tener flexibilidad suficiente para abarcar tecnologías híbridas, porque los que se centran expresamente en tecnologías específicas pueden obstaculizar la utilización de las tecnologías múltiples[310].

En nuestra opinión, al elaborar marcos jurídicos y normativos, para reglamentar el uso de métodos híbridos para la firma electrónica, se debería prestar atención a que su uso sea suficientemente flexible, porque lo que marcos normativos que se enfocan en tecnologías específicas, pueden obstaculizar la utilización de las tecnologías múltiples. La aceptación de estos criterios tecnológicos híbridos, facilitará mediante disposiciones neutrales respecto de las tecnologías, lo dicho anteriormente.

3.2.1.1.2. Firmas escaneadas o mecanografiadas

La inquietud, respecto del efecto, que las nuevas tecnologías pueden tener en la aplicación de normas de derecho concebidas para otros medios, ha conducido con frecuencia, a centrarse en tecnologías avanzadas, que hacen más seguros los métodos de autenticación y firma electrónicas[311].

En este escenario, suele perderse de vista que muchas de las comunicaciones mercantiles en el mundo, cuando no la mayoría, no utilizan ninguna tecnología concreta. En la práctica diaria, las empresas realizan intercambios de correos electrónicos sin ningún tipo de autenticación de identidad o firma, simplemente ponen

[309] CLIFFFORD NEUMAN, B.; TS´O, T.: "Kerberos: An Authentication Service for Computer Networks", *IEEE Communications Magazine*, septiembre, 1994, vol.32, núm.9, pág.33-38.
[310] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 64.
[311] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 65.

el nombre mecanografiado de la persona que realiza la comunicación, empresa y dirección de ésta, en otras ocasiones, se incrusta, en la comunicación electrónica, una copia digitalizada de la firma original manuscrita, con el fin de dar a ésta un aspecto más oficial, utilizando imágenes de firmas manuscritas reproducidas en facsímil o escaneadas.

Cuando el método utilizado, para la realización del contrato electrónico, es el correo electrónico, basta con tener una conexión a Internet y una cuenta de correo electrónico. Además, hay que tener presente el amplio margen de maniobra que otorga a los contratantes, ya que pueden expresar libremente las peticiones que quieran realizar.

Es común el pensamiento de que el nombre de la persona puesto al pie del correo electrónico como firma, no brinda seguridad ni sirve categóricamente para demostrar la identidad del iniciador de la comunicación electrónica. Sin embargo, las empresas deciden utilizar este tipo de transacciones en pro de la facilidad, economía y por su conveniencia.

Por ejemplo, pensemos que un correo electrónico es enviado por una persona autorizada en la empresa. La comunicación proviene de éste, cuando el e-mail ha sido enviado por el propio emisor, que es una persona autorizada para actuar en nombre del emisor, pues normalmente posee una cuenta de correo electrónico identificable. Por consiguiente, se puede decir que el sistema de información está bajo su autorización y que la firma electrónica empleada permite vincular al signatario con el mensaje electrónico y atribuir la autoría de éste. Por ello, este método podría tener la misma validez y eficacia probatoria, que la ley otorga a la firma autógrafa, siempre que llenen los aspectos previstos en la norma. Dicho lo anterior, en principio, se podría confiar en una dirección de correo electrónico de una empresa.

Pensemos, que un empleado tiene una dirección de correo electrónico. Esta dirección ha sido autorizada, para su uso dentro de lo que es el ámbito de la empresa, por un superior, que se la ha entregado con unas claves que están en su posesión. Esta cuenta se utiliza de manera efectiva diariamente y vincula a la empresa en determinados negocios jurídicos, a la vez que otorga una responsabilidad al empleado y, por éste, también a la empresa.

Al mismo tiempo, el correo electrónico, podríamos decir, que es el equivalente electrónico de un correo tradicional, de un fax o de un télex. Es bien sabido, que el destinatario de un fax recibirá una copia que tiene el nombre y/o número del remitente automáticamente, impreso en la parte superior junto con un tiempo de transmisión. Esto nos lleva a plantearnos la siguiente pregunta: ¿Puede decirse que el nombre que se genera automáticamente, por ejemplo, "antoniomerchan@typsa.es", o el nombre que se escribe al pie, como el número de fax del remitente que se plasma en el documento enviado, se puede considerar una firma identificando al remitente para el fin que se pretende?

Si el nombre es correcto puede que la respuesta dependa únicamente de si, el remitente sabía que el número o/y la dirección que aparece en el ejemplar son del destinatario. Tengamos en cuenta que una parte puede firmar un documento por el uso de su nombre completo o el apellido, precedido por alguna inicial o por todas sus iniciales o mediante el uso de un seudónimo o una combinación de letras y números, siempre que todo lo insertado en el documento, tenga como finalidad expresar, la intención del firmante y autenticidad del documento. Sin embargo, su inclusión puede que no haya sido la de concebir una firma para los fines que pretendía[312], por lo que un Tribunal puede tener dudas de que: si una de las partes crea y envía un documento en formato electrónico, con su nombre al final de éste, deberá constatarse si lo ha creado para vincularse con él o no.

En relación con la cuestión de si la inserción automática de una dirección de correo electrónico de una persona constituye una firma, debemos decir que tal circunstancias es un claro ejemplo de la inclusión de un nombre accesorio, en el sentido de que puede ser identificado por cualquiera de las partes, aunque puede haber ausencia de prueba de una intención contraria, pues la dirección electrónica se encuentra divorciada del cuerpo principal del texto del mensaje. A falta de pruebas en contrario, en nuestra opinión, no es posible sostener que la inserción automática de una dirección de correo electrónico sea una firma. Así, se ha pronunciado nuestro Tribunal Supremo al decir que "un el correo electrónico para que pueda otorgársele validez debe contener

[312] REINO UNIDO: Mehta v J Pereira Fernandes SA [2006] EWHC 813 (Ch).

una firma electrónica, en el supuesto contrario, se trata de un documento fácilmente manipulable"[313].

No obstante, si vemos el Artículo 3,5 de la Ley 59/2003 sobre Firma Electrónica, en su redacción actual, tras la modificación introducida por la Ley 56/2007, de Medidas de impulso de la Sociedad de la Información, de 28 de diciembre de 2007[314], nos dice, textualmente: "se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado", en concordancia con el Artículo 24,2 de Ley de Servicios de la Información y Comercio electrónico que nos dice que "en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental". De esta forma, el Tribunal lo valorará conforme a la sana crítica (Artículo 384 de la Ley de Enjuiciamiento Civil)[315].

Por otro lado, a la pregunta de si un nombre, en el sentido al que nos hemos referido anteriormente; es decir, con la intención de identificarse y dar autenticidad al texto, está escrito al final del mensaje puede considerarse una firma electrónica de manera efectiva y aún más si las comunicaciones se repiten entre mismas personas. ¿Por qué? Porque hay un reconocimiento de las partes, de la autenticidad de la identidad de la persona dentro del propio mensaje electrónico.

Siguiendo nuestra legislación, todo lo dicho cobra fuerza. A la firma electrónica no se le negarán efectos jurídicos, ni será negada como prueba en juicio, por el sólo hecho de no estar incorporada a un soporte digital (Artículo. 3,8 y 3,9 Ley 59/2003 firma electrónica y 5,2 de la Directiva). Lo anterior se completa con lo dispuesto en el Artículo 23,3 Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, según el cual "siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico", añadiendo el Artículo 24,1 que la prueba de la celebración de un

[313] ESPAÑA: Sentencia del Tribunal Supremo, número 756/2012, de 13 de diciembre (RJ 2013/1250), Fundamento de Derecho 7º.
[314] BOE de 29 de diciembre de 2007.
[315] ARMENTA DEU, T.: *Lecciones de Derecho Procesal Civil*, Madrid, 2010, págs.171 y ss.

contrato por vía electrónica, o el envío de información, y las obligaciones que tienen su origen en ambas se sujetará a las reglas generales del ordenamiento jurídico y, en su caso, a lo establecido en la legislación sobre firma electrónica. En todo caso, serán los Tribunales, de acuerdo con lo dispuesto en la Ley de Enjuiciamiento Civil, los que deberán de valorar los distintos medios de prueba según las reglas de la sana crítica (Artículo 326,2).

Es previsible que en la práctica de la prueba, en relación con la firma electrónica, tenga lugar, fundamentalmente, a través de la prueba de reconocimiento judicial y de perito[316]. En este sentido, el Artículo 356 LEC faculta al Juez para que pueda practicar en un solo acto ambas pruebas, pudiendo las partes también solicitarlo. Si éste fuera el caso, parece que, aparte de los hechos reflejados en el acta de reconocimiento judicial, el perito podrá realizar cuantas apreciaciones estime oportunas, que habrán de ser tenidas presentes por el juez, según las reglas de la sana crítica (Artículo 358 y 354 en relación con el Artículo 348 LEC)[317]. Es indudable que, salvo declaración claramente ilógica o contraria a las más elementales leyes de la naturaleza y de la posibilidad, la valoración del perito será determinante. Lo que está fuera de toda duda es que la Ley 59/2003 remite el valor probatorio de la firma electrónica a lo dispuesto en las leyes procesales. Así nos lo dice el Artículo 3,8 de la Ley de Firma Electrónica: "el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio", sin una clara alusión al formato de firma electrónica más simple. Así, si se impugna la firma, se estará a lo establecido en el Artículo 326 LEC.

En nuestra opinión, la Ley de Firma Electrónica 59/2003 soluciona el problema técnico de cómo tramitar la impugnación, de un documento en soporte electrónico; es decir, vía firma electrónica más simple, a través de la introducción de un nuevo apartado en el referido Artículo 326 LEC, el tercero, que expresamente remite a lo establecido en el Artículo 3 de dicha Ley. Así, cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a

[316] BONET NAVARRO, J.: *La prueba en el proceso civil: cuestiones fundamentales*, Madrid, 2009, págs. 167 y ss.
[317] FERNÁNDEZ-BALLESTEROS LÓPEZ, M. A.; RIFÁ SOLER, J. Mª. VALLS GOMBAU, J.: *Comentarios a la nueva Ley de enjuiciamiento civil: volumen II*, Barcelona, 2001, págs. 1537 y ss.

lo establecido en el Artículo 3 de la Ley de Firma Electrónica[318]. Por tanto, nos encontramos con la existencia de una norma procesal que se encuentra fuera de la LEC.

Este Artículo 326,3 LEC se refiere, en general, a los documentos electrónicos, sin especificar que se encuentren firmados o no, ni el tipo de firma; éste nos remite a los Artículo 3,8 y Artículo 3,9, que establecen que "no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación con los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica", que se remiten a las firmas electrónicas en general. De esta forma, como dice el Prof. Cruz Rivero, no se pueda extraer otra conclusión a la vista del Artículo 5,2 de la Directiva de Firma Electrónica, de cuya trasposición se encarga el Artículo 3,9, que se refiere a los aspectos jurídicos en general, sino también a los efectos probatorios, velando porque no se le niegue admisibilidad como prueba en los procedimientos judiciales a la firma electrónica simple por el mero hecho de que se presente en forma electrónica[319].

3.2.1.1.3. Firma digitalizada

La ISO (Organización Internacional de Normalización)[320] y la IEC (Comisión Electrotécnica Internacional)[321] forman un sistema especializado, para desarrollar normas internacionales voluntarias a nivel mundial. Los organismos nacionales, que son miembros de ISO e IEC, participan en el desarrollo de estas normas internacionales a través de sus comités técnicos, establecidos por la organización respectiva[322], para atender campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo, concretamente, en el ámbito de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto: ISO/IEC JTC 1.

---

[318] MARTÍN PASTOR, J.: "Los medios de prueba: interrogatorio de las partes" en *Derecho Procesal Civil* (Coord. Y Dir. Ortells Ramos, M.), Navarra, 2013, págs. 381 – 404.
[319] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, págs.323.
[320] ISO (International Organization for Standardization).
Disponible en: http://www.iso.org/iso/home.htm (última visita: 27/6/2014).
[321] IEC (International Electrotechnical Commission).
Disponible en: http://www.iec.ch/ (última visita: 27/6/2014).
[322] En España: Subcomité español AEN / CTN71 / SC37.
Disponible en: http://www.aenor.es/aenor/normas/ctn/fichactn.asp?codigonorm=AEN/CTN%2071 (última visita: 27/6/2014).

A través de la ISO/IEC 19794-7:2014(E)[323], parte actualizada de la ISO/IEC 19794, la ISO y la IEC han especificado formatos de intercambio de datos capturados, en base a la realización de firmas manuscritas, en forma de una serie temporal de varios parámetros, utilizando dispositivos como tabletas digitalizadoras o sistemas bolígrafo inteligente. Los formatos de intercambio de datos son de carácter genérico, ya que se pueden utilizar en una amplia gama de áreas de aplicación, haciendo que entren en juego signos escritos a mano o firmas manuscritas.

Esta parte de la Norma ISO/IEC 19794 contiene: una descripción de los datos que se pueden capturar; tres formatos de datos para describir la información capturada; un formato completo para uso general, un formato que permite recoger la información de forma comprimida y un formato compacto, sin compresión, orientado a su uso con tarjetas inteligentes cuando se puede prescindir de cierta información; y, por último, ejemplos de contenido de los registros de datos y uso práctico en materia de captura de información biométrica[324].

Cuando hablamos de firmas digitalizadas, nos estamos refiriendo a firmas manuscritas-electrónicas, que realizamos en tabletas gráficas en varios escenarios de uso, como en pagos con tarjeta de crédito. De esta manera, podríamos hablar de una firma manuscrita digitalizada, o lo que es lo mismo, una firma electrónica que se obtiene por medio de la captura de la firma manuscrita, utilizando dispositivos de captura móviles o fijos (por ejemplo, las denominadas *tablets*).

Por consiguiente, si tenemos en cuenta la aserción, de que la firma es el trazo peculiar, mediante el cual un sujeto consigna su nombre y apellido o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad; nos encontramos que la firma digitalizada tiene elementos que la asemejan a la firma manuscrita de manera más real, salvando las distancias en el ambiente digital en referencia a signos, claves o huellas, para enfocar el *animus probandi* que brinda autenticidad y confidencialidad a la información esbozada en el documento.

---

[323] ISO/IEC: *ISO/IEC 19794-7:2014 Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data*, Genova, 5 de febrero de 2014.
Disponible en: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55938 (última visita: 27/6/2014).

[324] ISO/IEC: *ISO/IEC 19794-7:2014 Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data*, Genova, 5 de febrero de 2014, pág.1.

La firma obtenida podría decirse que es, en principio, una firma electrónica simple; sin embargo, a esta firma se le incluyen datos biométricos del firmante, como puede ser: presión o velocidad, sistemas de seguridad que determine si esta firma es similar a la original, utilización de certificados electrónicos no aportados por el firmante, etc.

Lo característico de esta firma electrónica es que todo no se queda en una simple captura o escaneo de la firma manuscrita del usuario, para posteriormente, insertarla en el documento, sino que se capturan, generan y almacenan suficientes datos para revelar y garantizar la firma como un atributo del mensaje de datos que identifica al autor, garantiza la inalterabilidad de la misma, el momento en que se realizó la firma, la autenticidad, verificación por terceros y que dicha firma no puede ser reutilizada en documentos posteriores.

Dicho lo anterior, a día de hoy, vemos que, en la práctica, viene utilizándose este tipo de firma; por ejemplo, al recoger un paquete, al retirar efectivo en algunas entidades financieras y al pagar con tarjeta de cliente en algunos comercios o grandes superficies. En ambos casos, nos encontramos con una relación contractual previa, aunque: por un lado, respecto al primer caso, podrían plantearse dudas en relación con la protección de datos del usuario, respecto al almacenaje de datos que realiza la entidad que entrega al consumidor el paquete; y por otro, en el segundo caso, nos podemos encontrar ante una relación contractual previa que ha llevado a la entidad a poder escanear la firma dando seguridad, confianza e incluso comodidad al cliente. Los datos capturados se deben a una información previa, contenida en formato papel, que ha sido objeto de captura conforme a una serie de criterios de longitud, caracteres permitidos por el software, obligatoriedad y validación de datos, establecidos a través de un escaneo de éstos que viene a permitir y facilitar la consulta y resguardo de los documentos probatorios e identificativos, de la misma forma que si estuvieran en formato papel (por ejemplo, documentos archivados como la fotocopia del DNI o la firma del contrato que se hizo en el momento de la fidelización del cliente[325]). A la captura de datos, se le suma un registro biométrico como medio para identificar a una

[325] Nos Referimos, por ejemplo, al momento de contratar la tarjeta del Corte Inglés.

persona, basado en sus características técnicas, especificaciones y estándares para la captura, compresión y almacenamiento de fotografía, firma y demás documentos digitalizados, que evidencian, en algunos casos, una relación contractual previa, con el fin de evitar duplicidades en el registro de personas[326].

En cualquier caso, lo que se pretende es dar validez y eficacia jurídica a este tipo de firma, lo que inevitablemente nos lleva a medir su valor probatorio, con respecto a las Leyes. Dicho lo anterior, teniendo en cuenta las circunstancias que se presentan en relación con este tipo de firma, parece evidente que no nos encontramos ante una firma electrónicas ni avanzada ni reconocida, a la vista de las definiciones técnicas establecidas en los Artículos 3,2 y 3,3 de la Ley 59/2003 sobre firma electrónica. Lo que nos lleva a la "flexibilidad" del Artículo 3,1 que establece, lo que se entiende por firma electrónica, y que venimos denominando firma electrónica simple, desde un parámetro, más o menos, de neutralidad tecnológica. Por tanto, la firma digitalizada tendrá efectos jurídicos reconocidos respecto a su eficacia y aplicación, atendiendo al tipo del trámite o transacción para la que se utilice[327].

Por otro lado, si observemos las partes que intervienen en la transacción que se va a realizar, tenemos: quien firma el documento (suscriptor), quien o quienes necesitan verificar la firma (receptor-empleado de la entidad), quien testimonia que una firma digitalizada pertenece a una persona (la Entidad certificante), que va ser la misma que va controlar el sistema (Departamentos de informática de la entidad que ha contratado con el cliente). En este punto, podemos ver que, en el proceso de comunicación electrónica, para facilitar la comprensión de los roles asumidos en la gestión y seguridad, el sistema permite atribuir el documento a su autor (suscriptor) de manera fehaciente; pues es éste quien la realiza por sí mismo y permite a la Entidad comprobar si ha habido modificaciones en la firma, cuáles son y dónde están e incluso en qué

[326] No obstante, podrían incluir muchos más datos como: huellas dactilares, iris, datos propios de eDNI.

[327] Informe CORA Para la Reforma de las Administraciones Públicas (Publicado el 21/06/2013 por el Ministerio de Hacienda y Administraciones Públicas (MINHAP) NIPO: 630-13-106-7 (línea) y Ministerio de la Presidencia NIPO: 002-13-038-9 (línea): "El tipo de firma que se utilice de ser adecuada a los principios de proporcionalidad, simplicidad y movilidad".
Disponible en:
http://administracionelectronica.gob.es/pae_Home/pae_Biblioteca/pae_PlanesEstrategicos/pae_PE_ambito_Nacional.html#.U7EnYfnV_Eg (última visita: 30/6/2014).

momento se ha realizado la firma que ya existía en el tiempo. Todo va a girar respecto a la firma, no en relación con el documento[328].

3.2.1.1.4. Datos biométricos

A través de la medición biométrica[329] se trata la identificación de una persona en base a sus características fisiológicas o de comportamiento intrínsecos. Esta información es utilizada para autenticar y verificar datos con respecto a una persona que dice ser quien es, por comparación con las características, previamente, características proporcionadas y almacenadas.

La biometría comenzó a gestarse a finales de los años 90, cuando se empieza a ver la necesidad de crear interfaces comunes, así como formatos de datos conocidos. En agosto de 2002, se creó un Subcomité (SC37) dedicado a la Identificación Biométrica, dentro del Comité Conjunto ISO/IEC sobre Tecnologías de la Información (JTC1), en el seno de la Organización Internacional de Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC)[330].

El Comité Técnico Mixto (JTC1) de la ISO/CEI ha elaborado más de 30 normas internacionales sobre biometría. Los trabajos del JTC1 relativos a normas de biometría también los lleva a cabo su Subcomité 27 sobre Técnicas de Seguridad TI (que cubre protección de plantillas, seguridad de los algoritmos y evaluación de la seguridad), y su

[328] Las entidades consultadas, que llevan a cabo este tipo de firma electrónica, nos han comentado que la firma se gestiona en un sistema de "firma manuscrita avanzada digitalizada". El firmante que utiliza la firma digitalizada está en igual posición que la entidad que lo gestiona para demostrar si la firma capturada es o no la suya (por ese motivo dicen que se envía por correspondencia la factura escaneada que se genera automáticamente, pues: "Cuando se emplea el papel, es decir, se envía en papel la factura, poca gente duda de que la firma que se capturó es la suya y que esa copia generada es válida para el usuario y que este debe tenerla". No obstante, en algunas de las reuniones da la impresión de que las versiones iniciales de los sistemas que emplean las entidades financieras se diseñan para proteger a la propia entidad y dejan indefenso al usuario cuya firma se gestiona, sin que este tenga conocimiento de ello. Así, dan confianza a los usuarios de la propia entidad, que no piden DNI alguno, de que todo se gestiona adecuadamente y se cuida de que no sean "la parte débil" en el empleo de las tecnologías. Por ello, me sorprendió el uso reiterado de frases como: "A veces se sobreprotege al usuario, e insistimos en algunos principios como la simetría probatoria. Difícilmente, la propia entidad podrá ser acusada de "mala praxis", y será más viable ante los órganos jurisdiccionales si finalmente es preciso recurrir a ellos por alguna de las partes".

[329] MURAKAMI , T.; TAKAHASHI , K.: "A measure of information gained through biometric systems", *Image and Vision Computing*, 26 diciembre 2013.

[330] SÁNCHEZ REÍLLO, R.: "La normalización en el campo de la Identificación Biométrica", *Dintel*, septiembre, 2012, págs.142-143.

Subcomité 17 sobre Tarjetas e Identificación Personal. Otras vías de trabajo abiertas, dentro de los estándares más importantes, se encuentra la familia ISO/IEC 19794 sobre los Formatos de Datos de las Modalidades, la ISO/IEC 19795 sobre la Metodología de Evaluación, y la ISO/IEC 19784 sobre Interfaces de Programación (BioAPI).

En el seno de la UIT[331], los trabajos sobre biometría comenzaron, en 2001, bajo la responsabilidad de la Comisión de Estudio 17 del UIT que coordina estas actividades a través de todos sus Grupos de Trabajo. En particular, la citada Comisión es responsable del estudio de la gestión de identidad; es decir, los métodos técnicos adecuados para identificar a los individuos y proteger sus identidades. Se están intensificando los trabajos para abordar el nuevo reto que supone lograr una infraestructura, unos servicios y unas aplicaciones de red más seguros. Evidentemente, las aplicaciones de telecomunicaciones que utilizan terminales móviles y servicios de Internet requieren métodos de autentificación que no sólo proporcionen un elevado grado de seguridad, sino que sean convenientes para los usuarios. Hasta la fecha se han publicado más de 70 Recomendaciones UIT–T sobre seguridad.

Un ejemplo del desarrollo de la biometría lo encontramos en los pasaportes biométricos, que también permiten el uso de la tecnología de Identificación por Radiofrecuencia. Actualmente, más de 50 países lo utilizan, entre ellos España, que desde el día 28 de agosto de 2006, todos los pasaportes que se expiden por los equipos radicados dentro del territorio nacional corresponden al denominado pasaporte electrónico (e-pasaporte), el cual incorpora un chip embebido en su portada posterior que contiene el dato biométrico relativo a la imagen facial del titular del documento, además de los datos personales que se contienen en las líneas OCR de lectura mecánica. Desde el 28 de junio de 2009 se incorporan, además, las impresiones dactilares de los dedos índices de ambas manos, o los que, en su defecto correspondan.

Las formas más populares de tecnología biométrica son las huellas dactilares, escaneo de retina, geometría de la mano, reconocimiento de voz, digitalización de imágenes, etc. Así, la utilización de dispositivos biométricos supone captar una muestra biométrica, en forma digital, de algún rasgo biológico de una persona y a continuación

[331] Disponible en: http://www.itu.int/net/itunews/about-es.aspx (última visita: 23/3/2014).

se extraen datos biométricos de esa muestra para crear una plantilla de referencia. Se confirma la identidad de la persona a la que pertenece la muestra biométrica, o se verifica la autenticidad de las comunicaciones presuntamente originadas por esa persona, comparando sus datos biométricos con los almacenados en la plantilla de referencia[332].

Esta tecnología está ganando interés por parte de los gobiernos y de las empresas, debido a su mayor grado de seguridad, por entenderse que es más difícil de alterar o alterarse al tratarse de rasgos físico. No obstante, los datos biométricos no son infalibles. Deben ser analizados por un programa de software siendo prácticamente imposible que este programa sea perfecto y, por tanto, blindado a cualquier ataque. Esto es así, porque los sistemas biométricos establecen unos límites de tolerancia.

Por ejemplo, es famoso el caso de un japonés, aficionado a la criptografía, en el año 2002, describió varios métodos para saltarse sistemas de autentificación biométrica basados en huellas dactilares: usando cinta adhesiva con cianocrilato sobre huellas, gelatina, etc. Tanto es así, que fue capaz de crear una huella dactilar falsa utilizando gelatina, de tal manera que consiguió crear moldes lo suficientemente buenos como para engañar a los sistemas de verificación en un ochenta por cien de los casos[333].

No obstante, planes biométricos están siendo desarrollados en todo el mundo. Actualmente, se están elaborando normas en varios organismos nacionales e internacionales entre los que puede citarse, la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI) y el Sector de Normalización de las Telecomunicaciones de la UIT (UIT). Los consorcios industriales, también, crean normas que soportan los objetivos de sus miembros, mientras que los organismos especializados de las Naciones Unidas, tales como la Organización de la Aviación Civil Internacional (OACI) y la Organización Internacional del Trabajo (OIT), redactan normas en el marco de sus dominios específicos, que puede que no hayan sido abordados por otras organizaciones. En particular, la OACI es responsable de la normalización de documentos de viaje legibles por máquina, incluidos los pasaportes

[332] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 45.
[333] Noticia disponible en: http://www.elmundo.es/ariadna/2002/98/1024555057.html (última visita: 26/3/2014).

electrónicos, mientras que la OIT ha establecido directrices sobre documentos de identidad biométrica para navegantes[334].

3.2.1.1.5. Firmas digitales basadas en la criptografía de clave pública

Por firma digital[335] se entiende aquella que se obtiene mediante aplicaciones tecnológicas en la que se utiliza criptografía asimétrica; también, denominada sistemas de cifrado de clave pública, para asegurar la autenticidad de los mensajes electrónicos y garantizar la integridad de su contenido. La firma digital se presenta de muchas formas, por ejemplo, firmas digitales infalsificables, firmas ciegas y firmas digitales irrefutables.

Las firmas digitales se crean, usando un sistema de criptografía[336] asimétrica o de clave pública, de manera que una persona que disponga de la clave pública puede determinar si:

a) La transformación se realizó utilizando la clave privada del firmante que corresponde a la clave pública del firmante (autenticación).

b) Los datos del firmante no han sido alterados (integridad).

c) Enviar mensajes secretos a través de canales inseguros como Internet: utilizando la clave pública del destinatario, de conocimiento público, el remitente puede estar seguro de que sólo el destinatario, el tenedor de la clave pública, puede descifrar el mensaje (confidencialidad).

El uso de la firma digital, como medio de autenticación, está condicionado a la posibilidad de que el receptor tenga garantía de la autenticidad de la clave usada, para

[334] Disponible en: http://www.itu.int/net/itunews/issues/2010/01/05-es.aspx (última visita: 26/3/2014).
[335] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 32 y ss.
[336] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 26.

verificar la firma. Una firma digital verificada, con una clave pública, únicamente garantiza, que el mensaje ha sido firmado por el poseedor de la correspondiente clave privada, pero no garantiza la identidad del poseedor de la clave privada, que puede ser un poseedor ilegítimo[337]. Así pues, un juego de claves, usado para crear una firma digital, no tiene una intrínseca asociación con nadie, ya que el par de claves, pública y privada, no tiene asociación intrínseca con ninguna persona, es, simplemente, un par de números.

Por una parte, resulta necesario encontrar una forma segura de asociar a una persona en concreto al par de claves. Esta necesidad puede acentuarse a medida que partes ajenas, sin relación contractual previa, realizan transacciones de comercio electrónico importantes.

Por otra, la firma digital es emitida durante un periodo de validez concreto. Cuando el certificado caduca o se revoca la clave pública, pierde dicha validez, aunque el par de claves no esté en entredicho. Por ello, este tipo de firmas electrónicas requiere un sistema de gestión, para que la firma siga disponible a lo largo del tiempo[338]. La dificultad se encuentra en el riesgo de que los registros electrónicos, en los que se han incluido las firmas, puedan resultar ilegibles o poco fiables con el tiempo por problemas tecnológicos o por quedar obsoletos. Ante esta situación, la firma electrónica digital resultante plantea problemas transfronterizos importantes.

Ante la situación descrita, surgen los terceros en confianza[339]; es decir, los prestadores de servicios de certificación o autoridades de certificación, que es la parte en la que confían los usuarios, que podrían ser públicas o privadas, aunque en la mayoría de los países, esta función la realizan agencias gubernamentales. Así pues, suele darse, que estos prestadores de servicios de certificación estatal expiden certificados, únicamente, para respaldar firmas digitales utilizadas por la administración pública. Además, para emitir un certificado de confianza, otra autoridad de certificación, en este caso privada, debe tener un certificado válido y verificable de sí

[337] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 34 y ss.
[338] MATÍNEZ NADAL, A.; FERRER, J.L.: "El problema temporal del sistema de certificados en el comercio electrónico", *Revista de la Contratación Electrónica*, enero 2001, núm. 1, págs. 1 -23.
[339] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 34 y ss.

misma, para entrar dentro del propio sistema estatal, planteándose el problema de quién certifica a la autoridad de certificación; a la vez que se presenta inquietud por la relación de nivel jerárquica que pueda surgir entre ellas.

En este contexto, resulta esencial que el sistema de certificados se estructure de tal forma que resulten válidos e interoperables entre diversos países, ante la naturaleza transfronteriza del comercio electrónico, para que pueda darse un reconocimiento internacional de certificados.

El prestador de servicios de certificación es quien expide el certificado, que es un registro electrónico, en el que se indica la clave pública junto con el nombre del suscriptor de certificado, como sujeto del certificado y con el que puede confirmarse que el firmante potencia que figura en el certificado posee la clave pública correspondiente. De esta forma, el prestador resulta responsable de adoptar ciertas medidas para determinar la identidad de la persona, para la que emite un certificado. La regulación de la responsabilidad, de esta entidad, es muy importante por la posición que ocupa en el sistema de gestión; este régimen a la vez, resulta problemático en el reconocimiento transfronterizo, pues como veremos más adelante, los criterios que se adoptan en las diversas leyes son muy diferentes, ya que giran en torno al prestador.

3.2.1.1.5.1. Tarjetas inteligentes

Las tarjetas inteligentes[340] son aquellas que incluyen un chip informático que almacena información la cual puede ser modificada. Con ellas, se trata de identificar a los usuarios utilizando sistemas capaces de ejecutar algoritmos criptográficos.

En los últimos años ha habido una creciente demanda de tarjetas inteligentes de clave pública, especialmente, en las administraciones públicas. De esta forma, en un

[340] SIDDHARTHA, A.: "National e-ID card schemes: A European overview", *Information Security Technical Report*, mayo, 2008, vol. 13, núm. 2, págs.46-53.

estudio emprendido por la OCDE[341] se identificaron los países[342] que han realizado activamente estrategias nacionales relacionadas con la gestión de la identidad.

Por consiguiente, se observa que se han puesto en marcha campañas nacionales de distribución de tarjetas de identidad física, dotadas de un "chip" que contiene los datos que necesita un ciudadano para producir una firma digital. Nos encontramos con que se ha hecho habitual, la distribución de dispositivos de firma electrónica digital y que, además, llegan a almacenar, en algunos, casos datos biométricos, a menudo, en forma de tarjetas de memoria, en el contexto de iniciativas de gobernación electrónica.

a) Alemania

En Berlín, el 3 de Abril de 2003, se realiza una "Declaración de asociaciones público-privadas para promover el uso de firmas digitales", en ella se recoge la forma de emitir certificados con mucha más facilidad. A ello, hay que añadir el objetivo de esta Declaración: promover el uso de tarjetas inteligentes para firmas reconocidas y avanzadas dentro de Alemania. Esta declaración fue añadida a la Ley de firma electrónica de 2001, en 2005.

Los promotores de la Declaración fueron el Ministerio Federal de Economía y la Oficina Federal para la Seguridad de la Información, que trabajaron conjuntamente con los principales actores del sector privado, para desarrollar la Firma Industrial de Interoperabilidad y de Especificación Estándar, denominada con las siglas ISIS, que especifica formatos estandarizados, para datos y mensajes, que se aplican a los servicios prestados en virtud de la Ley de Firma Digital alemana y el Marco Europeo[343].

---

[341] OCDE: "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, 2011 núm.196, pág.20.
Disponible en: http://www.oecd.org/sti/ieconomy/49338380.pdf (última visita: 22/4/2014).

[342] Entre ellos se encuentran: Alemania, Australia, Austria, Canadá, Chile, Dinamarca, Eslovenia, España, Estados Unidos de América, Italia, Japón, Luxemburgo, Nueva Zelandia, Países Bajos, Portugal, República de Corea, Suecia y Turquía.

[343] M'CHIRGUI, Z.: "Smart card industry: a technological system", *Technovation Review*, núm.25, 2005, pág.929–938.

Los objetivos de la iniciativa están dirigidos a construir una infraestructura común para las aplicaciones de comercio electrónico y gobierno electrónico, utilizado las firmas digitales en un formato basado en tarjetas inteligentes[344]. Se trata de crear una infraestructura robusta para la prestación de servicios en línea, en el ámbito de la administración pública y la realización de transacciones comerciales y financieras de una forma segura.

En este entorno, nace la tarjeta de identificación que viene a cumplir esencialmente tres funciones[345]: primero, la tarjeta está equipada con un chip RFID sin contacto, en el se guardan los datos biométricos faciales y datos dactiloscópicos. Con esta tarjeta, el titular de la tarjeta obtiene un equivalente funcional a la tarjeta de identificación existente en el mundo físico. Segundo, la tarjeta de identificación servirá como dispositivo seguro de creación de firma, en el sentido del Artículo 2,10 de la Ley alemana sobre las Firmas Electrónicas (Signaturgesetz), ofreciendo así la posibilidad de generar firmas electrónicas reconocidas. Esta función de la tarjeta de identificación alemana es opcional y tiene costes adicionales. El enfoque está basado en el mercado alemán, por ello, en lo que respecta al mercado de los proveedores de servicios de certificación, no será alterado; es decir, los certificados reconocidos de las tarjetas de identificación oficial alemana se emitirá por proveedores privados. Tercero, la prueba de la identidad electrónica, es una parte estándar de cada tarjeta de identificación.

La nueva tarjeta, inteligente de identidad nacional alemana, está siendo comercializada como una forma de promover el comercio a través de Internet. Los titulares de las tarjetas pueden activar la función de comercio y tener una firma electrónica en el chip, de manera opcional, lo que lleva un coste al ciudadano, que supone mantener la libre competencia entre entes públicos y privados.

De esta forma, si un proveedor de servicios desea permitir el uso de la tarjeta de identidad alemana, el proveedor de servicios interno sólo tendrá que solicitar un certificado de autorización al gobierno alemán, que lo incorporará a su registro. Sólo con este certificado se le permitirá, al proveedor de servicios, prestar servicios de

[344] NOTICIA SCIENCE DIRECT: "German ID card to promote e-commerce", *Card Technology Today*, Julio – agosto, 2008, vol.20, núm.7, pág.3.
[345] SIDDHARTHA, A.: "National e-ID card schemes: European overview", *Information security technical report*, mayo, 2008, vol. 13, núm.2, pág.46-53.

certificación en Alemania y obtener información acerca de los datos de carácter personal contenidos en el chip del titular. Para que la información sea transmitida a través de Internet deberá introducir su PIN en el lector de tarjetas conectado al PC del titular de la tarjeta; además, de un dispositivo de comercio electrónico. Asimismo, se aprecia como la tarjeta, no sólo facilitará el comercio por Internet y la banca en línea, sino también el gobierno electrónico y, con ello, la tramitación de los procedimientos administrativos en línea. En este sentido, la OCDE ha calificado la actual Ley alemana de firma electrónica, atendiendo a las barreras del comercio internacional, como una Ley basada en estándares, que hace que la gran mayoría de las barreras existentes puedan ser prácticamente descartadas[346].

b) Italia

En Italia se empezó a planificar la introducción del DNI electrónico en 1999[347]. Éste e-DNI se recoge en el Artículo 66 del Decreto Legislativo sobre firma electrónica italiano, abordando dos tipos de tarjetas de identificación electrónica: el e-DNI y el Documento Nacional de Servicios.

El DNI electrónico[348], que es realizado por la Casa de la Moneda, es un instrumento de identificación personal y de autenticación, para el acceso a los servicios web, proporcionados por las administraciones públicas. Las reglas técnicas de este documento de identidad personal se han indicado en la Orden Ministerial de 8 de noviembre de 2007[349].

Este documento electrónico contiene todos los datos de identificación y la información oficial sobre la persona. Asimismo, contiene datos que son almacenados en

[346] OCDE: *The use of authentification across Borders in ORCD Countries*, Paris, 2005, pág.12.
[347] TELECOMICATIONS POLICY: *How advanced are Italian regions in terms of public e-services? The construction of a composite indicator to analyze patterns of innovation diffusion in the public sector*, 28 de febrero de 2014.
Disponible en: http://www.journals.elsevier.com/telecommunications-policy/ (última visita: 2/4/2014).
[348] Disponible en:
http://www.comune.viareggio.lu.it/index.php?option=com_content&view=article&id=216&Itemid=143 (última visita: 26/3/2014).
[349] Disponible en:
http://www.interno.gov.it/mininterno/site/it/sezioni/servizi/legislazione/enti_locali/0997_2007_11_08_Decreto_8_novembre_2007.html (última visita: 22/4/2014)

un microchip y en una banda óptica: la información personal, número de seguridad social, los datos de residencia, la ciudadanía, el código numérico de la ciudad de emisión, fecha de emisión y fecha de vencimiento, así como la firma del titular, la fotografía. También puede contener datos administrativos del Servicio Nacional de Salud, y toda la información necesaria para utilizar la firma digital.

En papel, para proteger la seguridad del ciudadano, se le expide al mismo un código secreto personal (PIN), con una secuencia de números secretos y personales que permiten la identificación del usuario; y un el código PUK para desbloquear el PIN en caso de que el ciudadano escriba mal su número PIN tres veces o se olvide de éste. Si la tarjeta se pierde o es robada, con el fin de garantizar la integridad de los datos y su privacidad, el Centro Nacional de Demografía Servicios (CNSD), a través del Ministerio del Interior[350], asegura y garantiza el sistema de gestión unificando la emisión del certificado, con completa funcionalidad, transparencia y seguridad de los procesos de los registros de autenticación y validación.

Por otro lado, se emite el Documento Nacional de Servicios (CNS) [351], que es una tarjeta inteligente para iniciar una sesión en los servicios en línea de la administración pública en todo el territorio nacional. El CNS es una innovación importante para realizar actuaciones entre los ciudadanos y la Administración Pública. Se trata de una tarjeta o dispositivo que contiene un certificado digital de autenticación persona, que posee una herramienta de software, que facilita la identificación de los usuarios en la red y le permite navegar por la web, a los ciudadanos italianos, a través de los certificados digitales facilitados por el gobierno, por ejemplo, para acceder a los registros médicos, en el sitio web de la autoridad de salud local. No contiene foto del titular y no necesita requisitos adicionales de seguridad. Por ello, la identidad electrónica completa de los ciudadanos se compone de esta tarjeta y el DNI electrónico, lo que garantiza la interoperabilidad para actuar con todas las administraciones.

Esta tarjeta es emitida por una autoridad de certificación reconocida. Esta autoridad adquiere la función de certificadora al cumplir los criterios de autorización

[350] Disponible en: http://www.interno.gov.it/mininterno/site/it/temi/servizi_demografici/scheda_006.html (última visita: 2/4/2014)
[351] Disponible en: http://www.card.infocamere.it/infocamere/pub/faq_1905 (última visita: 26/3/2014).

establecidos en la Decreto Legislativo sobre firma electrónica italiana. La lista de autoridades de certificación se publica anualmente[352], en la que se puede apreciar un claro predominio de autoridades públicas. Este certificado emitido debe ser aceptado por cualquier administración, lo que permite la interoperabilidad entre las administraciones y, a la vez, permite acelerar la forma de autenticación y garantizar la validez de la información contenida en el certificado. Tiene un tiempo de validez determinado, fuera de la cual se considera no válida.

c) España

El DNI electrónico fue uno de los objetivos del Gobierno, manifestado en el Plan Info XXI[353]. Con la Ley 59/2003 de Firma Electrónica se cumplió este objetivo al establecerse, como gran novedad, en los Artículos 15 y 16, las bases para la regulación del Documento Nacional de Identidad electrónico, cuya implantación pretendía ser un avance sustancial en el desarrollo de la Administración y el comercio electrónico.

La normativa referente al DNI ha sido desarrollada por el Real Decreto 1533/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica y por la Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior relativa a los certificados de firma electrónica, incorporados al Documento Nacional de Identidad.

Con el DNI electrónico se pretende poner a disposición de los ciudadanos certificados reconocidos, que garanticen digitalmente su identidad y proporcionen la posibilidad de firmar documentos electrónicos. De esta forma, prevé la incorporación de las facilidades de identificación y firma electrónica al DNI para que éste pueda

[352] De acuerdo con la normativa vigente, la AgID publica en su página web la lista las autoridades de certificación en formato HTML, la lista se hace en conformidad con la norma ETSI TS 102 231. La lista se encuentra publicada en: https://applicazioni.cnipa.gov.it/TSL/IT_TSL_CNS.pdf (última visita: 4/4/2014).

[353] TOMÉ MUGURUZA, B.: "El plan de acción info XXI: la sociedad de la información para todos", LA *Estrategia de impulso: economía industrial*, 2001, núm.338, págs.19-23.

utilizarse en el ámbito telemático, para identificar a su titular y permitir firmar por medios electrónicos[354].

El Artículo 15,1 de la Ley nos define el DNI electrónico como "el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos". Por otra parte, el apartado 2 de este Artículo, impone la obligación de que todas las personas físicas o jurídicas, públicas o privadas, deben reconocer la eficacia de este DNI, para acreditar su identidad y los demás datos personales del titular que consten en el mismo y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Así, observamos que a través del DNI se pretende dotar a los ciudadanos de una tarjeta de identificación, que recoja las menciones básicas del sujeto y, al mismo tiempo, se configura como un mecanismo generador de firmas de obligatoria aceptación, por todos los sujetos del tráfico jurídico.

Ante esto, no hay duda de que, la implantación del DNI electrónico, supone un medio para dar seguridad a las transacciones de comercio electrónico, a la vez que se considera fundamental para el desarrollo de la administración electrónica. Así, ante el posible uso administrativo y comercial del DNI electrónico, nos encontramos de frente con el principio establecido en la Directiva de libre prestación de bienes y servicios de firma electrónica, principio también recogido en el Reglamento de identificación electrónica.

Lo que nos lleva a la obligatoria crítica de la regulación que la Ley contiene, al suponer un claro ataque a la libre prestación de servicios de certificación, eliminando cualquier posibilidad de libre competencia por parte de las empresas prestadoras de servicios de certificación privadas, encontrándonos, una vez más, con una clara invasión competencial del mercado por parte del sector público[355].

---

[354] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica*, Madrid, 2009, págs.276 y ss.

[355] ALAMILLO DOMINGO, I.; URIOS APARASI, X: "Comentario crítico de la Ley 59/2003", *Revista de la Contratación Electrónica*, febrero, 2004, núm.46, págs.3-64.

Su expedición es competencia atribuida al Ministerio del Interior, estableciendo que los órganos del ministerio que asuman tal función, en tanto que implica la expedición de certificados reconocidos, y su actuación como autoridad de certificación, deberán cumplir todos los requisitos que la Ley 59/2003 impone a los prestadores emisores de certificados reconocidos.

De esta manera, se aprecia, de forma aún más clara, la invasión del mercado por parte del sector público aprovechándose de su posición, al establecer una reserva competencial conectada con la identificación de los nacionales españoles[356], problema que se plantea de forma generalizada en todos los Estados miembros UE.

Por ello, la existencia de un DNI electrónico válido para todo tipo de usos, teniendo en cuenta que de *facto* se utiliza para todo, resulta un inconveniente para los prestadores de servicios de certificación privados, que se dedican a la emisión de certificados como actividad empresarial. Esto es así, debido a que en el mercado español van a coexistir, sí o sí, dos operadores con una clara posición dominantes[357]: la Fábrica de Nacional de Moneda y Timbre y el DNI electrónico, medio de identificación obligatorio para todos los ciudadanos españoles mayores de 14 años.

Al mismo tiempo, el DNI tiene la doble función de identificar de una forma tradicional y a la vez en el entorno electrónico[358]. Esta dualidad se refleja en las características de la tarjeta soporte, prevista en el Artículo 10 del RD 1553/2005, como en el contenido de la tarjeta, previsto en el Artículo 11 de mencionado RD.

Conforme al Artículo 10 la tarjeta en soporte material lleva incorporado un chip electrónico que posibilita las mencionadas utilidades informáticas del DNI. El chip contendrá:

[356] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica*, Madrid, 2009, págs.282 y ss.
[357] CRUZ RIVERO: "El DNI electrónico y el mercado de entidades de certificación", *Revista Electrónica de la Contratación*, 2006, núm.69, págs.21-56.
[358] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica*, Madrid, 2009, págs.292 y ss.

a) Los datos personales de su titular digitalizados (filiación del titular, imagen digitalizada de la fotografía y de la firma manuscrita, así como impresión dactilar del dedo índice de la mano derecha).

b) El certificado, reconocido, de autenticación y de firma electrónica del titular.

c) El certificado de la autoridad emisora, que contiene la clave pública de la misma.

d) Las claves privadas necesarias para la activación de los certificados.

Los certificados emitidos no tienen una validez indefinida, según el Artículo 12 del Real Decreto, la vigencia de los certificados reconocidos es de 30 meses, resultando su vigencia inferior a la del propio DNI, que tiene una validez de 5 o 10 años. Razón por la cual este mismo dispone que pueda solicitarse la expedición de nuevos certificados que se incorporaran a la nueva tarjeta. Una vez finalizado el plazo de vigencia del certificado causará baja y por tanto su revocación.

Llama la atención que la validez del certificado es distinta, no sólo de los certificados electrónicos reconocidos emitidos conforme a otros ordenamientos jurídicos, sino también respecto al régimen previsto en el Artículo 8,2 de la Ley 59/2003, que dice que "el periodo de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este periodo no podrá ser superior a cinco[359] años". Lo que puede hacer dudar respecto a su seguridad.

d) Estados Unidos

[359] Disposición final 6 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, modifica el Artículo 8,2 de la Ley 59/2003 respecto al periodo de validez de los certificados electrónicos reconocidos, pasando de cuatro a cinco años (BOE-A-2014-4950).
Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950 (última visita: 9/12/2014).

En EEUU[360] fue aprobada, en mayo de 2005, la *REAL ID Act*[361], que crea una tarjeta de identificación nacional de facto. Ésta se adjuntó a un proyecto de ley sobre víctimas del tsunami y de los créditos militares, y pasó con poco debate y sin audiencias. Aparentemente es voluntaria, aunque se quiere establecer la obligatoriedad de que todas las personas la tengan en su posesión, de hecho se pretende convertir la licencia de conducir en un sistema nacional de identificación, proyecto que ha quedado estancado durante años ante la resistencia férrea de algunos Estados.

Esta Ley trata de imponer estándares tecnológicos y procedimientos de verificación de la identidad, que incluyan algunas protecciones para la privacidad individual y la seguridad. De esta forma, se considera que va más allá de la capacidad actuar de los gobiernos federales y de la voluntariedad, que un principio, inspira la propia Ley, pues, la *REAL ID Act*, obliga a los trabajadores y funcionarios federales de inmigración, ya que deben verificar el estatus de ciudadanía; asimismo pretende crear normas nacionales para crear tarjetas de identificación, que puedan ser utilizadas a bordo de aviones comerciales y para el acceso a determinados establecimientos federales.

Con fecha de 20 de enero de 2014, el Departamento de Seguridad Nacional anunció en qué fase de aplicación se encontraba la Ley, en un nuevo intento de impulsar la licencia de conducir en sistema de identificación, planteando como plazo de ejecución 2017, nueve años después de la fecha límite para su establecimiento, que estaba previsto para 2008. Con este anuncio se comunicó, también, que, desde la aprobación de la Ley *REAL ID* de 2005, varios Estados habían aprobado leyes rechazando el sistema de identificación nacional[362], al considerar que el sistema que se pretende imponer a través de la *REAL ID Act* perjudicaría más que protegería a los

[360] España ayudará a Estados Unidos a desarrollar su DNI electrónico.
Disponible en: http://www.red.es/redes/ (última visita: 4/4/2014).
[361] REAL ID Act of 2005, Pub. L. 109-13, 119, Stat. 302, publicada el 11 de mayo de 2005.
Disponible en: http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/html/PLAW-109publ13.htm (última visita: 4/4/2014).
[362] Hay 14 estados en clara situación de incumplimiento: Alaska , American Samoa , Arizona , Kentucky, Louisiana , Maine, Massachusetts , Minnesota , Montana , Nueva Jersey , Nueva York, Islas Marianas del Norte , Oklahoma, Utah y Washington. De la misma manera hay una lista de 21 estados en la actualidad que cumplen con los estándares de la ley REAL ID de 2005 para las licencias de conducir y tarjetas de identificación. Estos estados son Alabama , Colorado , Connecticut , Delaware , Florida , Georgia , Hawaii , Indiana , Iowa , Kansas , Maryland , Mississippi , Nebraska , Ohio, Dakota del Sur, Tennessee , Utah , Vermont , Virginia Occidental, Wisconsin y Wyoming.

ciudadanos de la privacidad y la seguridad en la red, consiguiendo exacerbar el problema del robo de la identidad[363].

En oposición frontal a la Ley se sitúa la *Electronic Privacy Information Center* (EPIC)[364], que en un análisis detallado explicó que, el sistema realizado por el Departamento de Seguridad Nacional en la *REAL ID*, incluye pocas protecciones para la privacidad individual y la seguridad, en su base de datos nacional de identificación, pues daña la seguridad nacional mediante la creación de un nuevo marco de "confianza" que da más facilidad a los delincuentes.

La EPIC instó a buscar un modelo alternativo, en torno a un sistema de identificación descentralizado, que reduzca los posibles riesgos asociados a las brechas de seguridad y mal uso de la información personal. Busca, a través de la innovación tecnológica, permitir el desarrollo de identificadores interdependientes, en el mismo sentido marcado por la ABA con la Identidad Federada. Así pues, considera que, un enfoque descentralizado de la identificación, habilita la autenticación sin riesgo, dentro de un sistema de identificación universal. Por consiguiente, si hay peligro, no todos los identificadores se echan a perder y los ladrones de identidad no pueden acceder a todas sus cuentas, pues el sistema puede cerrarse con más facilidad ante cualquier riesgo. Todo ello permitiría que cualquier sistema pudiera ser compartido mejorando la seguridad y la confianza[365].

e) Corea del Sur

En 1996, el Gobierno de Corea del Sur puso en marcha un ambicioso plan, basado en las tarjetas de identificación electrónica, que permitirían una administración más

[363] HOMELAND SECURITY: *REAL ID enforcement in brief*, 5 de febrero de 2014. Disponible en: http://www.dhs.gov/sites/default/files/publications/real-id-enforcement-in-brief-20140205.pdf (última visita: 4/4/2014).
[364] ELECTRONIC PRIVACY INFORMATION CENTER: *REAL ID implementation review: few benefits, staggering costs. Analysis of the department of homeland security's national id program,* mayo, 2008, págs.3 y ss.
[365] ELECTRONIC PRIVACY INFORMATION CENTER: *Real id implementation review: few benefits, staggering costs. Analysis of the department of homeland security's national id program electronic privacy information center*, mayo, 2008, pág. 10.

efectiva de los datos personales. Esta tarjeta de identificación era una tarjeta inteligente que tenía instalada un chip que contenía una gran cantidad de datos personales[366].

Las voces críticas empezaron a florecer cuando, la imagen utópica de una sociedad digital, comenzó a fallar ante los robos de identidad que empezaron a sucederse. Los defensores de las tarjetas insistían en los aspectos positivos como la reducción de costes, la eficiencia administrativa y mejores servicios sociales. Sin embargo, los críticos trataron hacer ver los problemas de invasión de la privacidad, el abuso de los datos personales y la degradación de los derechos humanos informáticos, control externo, etc.

La oposición y muchos sectores de la sociedad se levantaron, contribuyendo a enunciar los efectos negativos de la tarjeta de identificación electrónica. En un libro de consulta, una Asociación denominada "Red Progreso" describió la lucha en contra de la propuesta del gobierno australiano para una tarjeta nacional de identidad, llamada 'Tarjeta australiana" (Red de Progreso, 1997)[367].

Ante las voces críticas desde el sector civil, el Gobierno trató de influir en la opinión pública, realizando revisiones de la normativa. Sin embargo, la campaña anti-tarjetas destrozó todos estos intentos gubernamentales, debido a la creciente presión de los grupos de acción y el empeoramiento de las actitudes del público.

El Gobierno, en 1998, decidió aplazar la introducción de la tarjeta de identificación electrónica para 2000, pero finalmente, en febrero de 1999, abandonó el proyecto[368]. De esta forma, el Gobierno de Corea del Sur, que había completado la instalación de una base de datos nacional, compuesta por una selección de los datos

[366] SUK-LEE, K.: "Surveillant institutional eyes in South Korea: from discipline to a digital grid of control, the information society", *The Center for Interdisciplinary Research (ZiF*), 10- 11 febrero de 2006, págs. 119-124.

[367] En Australia han surgido asociaciones en contra de las tarjetas de identificación electrónica. Una de las principales es la EFA, una sociedad sin ánimo de lucro que ha mostrado su preocupación por los distintos intentos para imponer la denominadas tarjetas inteligentes, con un número único de identificación personal, vinculado a una base de datos centralizada que contenga una cantidad de datos de identificación personal sin precedentes de todos australianos y australianas.
Disponible en: https://www.efa.org.au/Issues/Privacy/accesscard.html (última visita: 23/4/2014).

[368] MUN-CHO KIM:" Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea" *International Sociology*, junio, 2004, págs.193-213.

personales de toda la población, incluyendo fotografías en color y huellas dactilares, se vio obligado a poner fin a su plan.

El plan de tarjeta de identificación electrónica se consideraba, como una forma de permitir, una inspección más eficaz de la vida de los ciudadanos, dado que el DNI electrónico se había diseñado para ser obligatorio y, por tanto, tendía a facilitar mecanismos de "etiquetar" a la ciudadanía, a través de la vigilancia de datos, sin protegerlos ante posibles riesgos de robos de tarjetas de identificación, crímenes informáticos, etc.[369].

En la actualidad, la idea del plan nacional del DNI electrónico ha sido totalmente desechada, siendo improbable que la propuesta nacional sobre tarjetas de identificación, vuelva a aparecer en un futuro próximo, ante el rechazo mostrado. La propuesta nacional se pierde en un ambiente caracterizado por la protección de la privacidad absoluta contra el ambicioso proyecto de convertir a Corea del Sur en un país digital líder[370].

3.2.2. El registro en el sistema de identificación

Como hemos observamos, a veces, en base al principio básico de los sistemas de gestión de la identidad, cada sistema que gestiona una identidad vinculada a un sujeto a su registro, pudiendo resumirse de la siguiente manera: un usuario se presenta a una autoridad de certificación o no, identificándose, bien mediante su certificado digital o un DNI o rellenando un formulario o enviando un correo electrónico (para la obtención de un correo electrónico se rellena un formulario previo o incluso el receptor del correo identifica al remitente en virtud de la buena fe negocial); entonces, la autoridad de confianza verifica la identidad del usuario y le da una identificación, la cual tendrá que ser presentada por el usuario, cuando desee utilizar el servicio.

[369] SUK-LEE, K.:"Surveillant institutional eyes in South Korea: from discipline to a digital grid of control, The information society", *The Center for Interdisciplinary Research (ZiF*), 10- 11 febrero de 2006, págs. 119-124.
[370] MUN-CHO KIM:" Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea" *International Sociology*, JUNIO, 2004, págs.193-213.

Si asumimos que cada sistema aplica estas medidas para facilitar algún servicio, observamos que la comprobación de la identidad es esencial, de tal manera que si esta comprobación de la identidad del usuario es errónea o si la prestación del servicio queda en una falsedad, se pone en peligro el sistema y con ella la fiabilidad del propio comercio electrónico.

Al final del proceso de identificación estarán, como sabemos, los datos recogidos y consignado en el documento electrónico de identidad, que se conoce como credencial de la identidad. De esta forma, como hemos comentado anteriormente, se trata de algo que una persona sabe (contraseña, PIN), posee (tarjeta inteligente, e-DNI, pasaporte), o es (datos biométricos), factores esenciales en el conocimiento y en la posesión, que requieren que la persona que se va a autenticar ante un sistema, recuerde o lleve consigo el dispositivo que le identifica.

Con el fin de comprender lo que la identificación y su autenticación implican, así como su importancia en las transacciones, es necesario repetir las funciones del sistema de gestión de la identidad. Por ello, con el registro se realiza una doble pregunta, que hemos hecho antes por separado; pero que en el sistema, se realiza de forma consecutiva: "¿quién es usted? y ¿cómo puede probarlo?".

La capacidad, para dar una respuesta fiable y creíble a esas preguntas, se ha convertido en un requisito decisivo de las actividades del comercio electrónico, especialmente, a medida que aumenta la importancia y la confidencialidad de ese tipo de transacciones. Apoyándose en las respuestas a esas dos preguntas, la parte en una transacción en línea puede decidir si procede o no a efectuar la transacción, es decir, si procede o no a autorizar o autenticar la transacción, que veremos en el siguiente Capítulo. Por ejemplo, la parte que procede a realizar la transacción va a decidir si celebra un contrato con la otra parte, si le permite el acceso a una base de datos confidencial o si le otorga algún otro privilegio[371].

[371] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 3.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita: 26/3/2014).

Hoy en día, existen una gran variedad de registros, tanto públicos como privados, con un claro predominio de los públicos sobre los privados, pues, son los Gobiernos de los distintos Estados los que tratan de controlar la validez de la identidad de cada persona. Obsérvese también, que las leyes de firma electrónica se han fijado casi en exclusiva en los métodos de autorización de la transacción, estableciendo requisitos técnicos a las firmas electrónicas.

En definitiva, con la evolución de la tecnología se están creando grandes archivos electrónicos, con ello grandes bases de datos comerciales y estatales. Un identificador nacional, contenido en una cédula de identidad, permite capturar información sobre una persona, que se halla en diferentes bases de datos, con el fin de que ellas puedan ser fácilmente enlazadas y analizadas a través de determinadas técnicas de análisis de datos. De la misma manera que las cédulas de identidad también se están volviendo "más inteligentes".

A pesar de lo anterior, las personas físicas o jurídicas pueden recurrir a diversos prestadores de servicios de identificación, ya sean públicos o privados. Cuando una persona se inscribe en uno de ellos para utilizar dichos servicios y crear una identidad electrónica; el problema surge en que una sola identidad no puede asociarse a diversas cuentas, ya que no conectadas entre sí, por cuestiones relativas a la prescripción tecnológica correspondientes a cada aplicación y a cada plataforma que se use.

Por otro lado, la generación de los datos tiene, además, la virtualidad de ofrecerse en un medio donde pueden pasar a ser directamente tratados. De esta forma, se crean archivos susceptibles de cruce y estructuración, así como de cesión y uso comercial. Por esta razón, hay que poner especial atención ante cualquier sistema de gestión de la identidad, pues estos normalmente implican una la colección; por ejemplo, un proveedor de identidad y la revelación a un usuario de confianza, de cierta información personal acerca de un sujeto individual.

Además, las transacciones de identidad también pueden facilitar el seguimiento de las actividades de un individuo, generando información personal adicional. Por lo tanto, la gestión de identidades presenta un nuevo desafío a la privacidad, en la que la transferencia de la información de identidad personal ocurre entre las organizaciones,

así como entre el individuo y la organización. Habrá, pues, que analizar en cada caso si estos datos adquieren la condición de personales, y por tanto, están sometidos a la legislación sobre datos personales.

3.2.3. Apuntes finales a la identidad electrónica

Como puede apreciarse, hay numerosas Leyes y reglamentaciones en relación con los sistemas de identidad, que muestran una gran variedad de métodos de autenticación. Sus diferencias, ante el carácter internacional que poseen en el comercio electrónico, plantea una situación jurídica sujeta a deberes y obligaciones, donde los Estados son libres a la hora de utilizar o introducir, a efectos de identificación electrónica, los medios que consideren necesarios; de la misma manera que establecen quien puede o no intervenir en el sector público o privado, en la prestación de estos medios. Sólo cuando nos movemos en el ámbito de la Unión Europea, gracias al Reglamento (UE) Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, se puede hablar de armonización legislativa, intentando obligar a los Estados miembros a decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional, para el acceso al menos a los servicios públicos en línea o a servicios específicos.

En definitiva, se trata de establecer ciertas condiciones, en relación con qué medios de identificación electrónica, que permitan aplicar el principio de reconocimiento mutuo, siempre que los niveles de seguridad de la identidad correspondan a un nivel igual o superior al exigido para el servicio en línea de que se trate.

El reconocimiento mutuo debe referirse, únicamente, a la autenticación a efectos de un servicio en línea, en tanto que ésta se encuentra en relación directa con la identificación, en el sentido de que la identificación no tiene utilidad a menos que la otra parte tenga capacidad para autenticarla.

Desde este punto de vista, se muestra la importancia de la atribución del mensaje al supuesto iniciador y la importancia de la idoneidad del método de identificación usado por las partes, para cumplir los requisitos de forma, en particular los requisitos exigidos en las propias leyes estatales.

De esta forma, como hemos comentado, ante la gran variedad de métodos de autenticación, se hace necesaria la no petrificación del reconocimiento legal de la autoría de la firma a los requisitos legales, exigidos con el establecimiento de estándares bien definidos tecnológicamente, como es el caso de Europa. Se trata, pues, del establecimiento de presunciones que nos lleven a una fiabilidad adecuada, para permitir la autenticación de la identidad del documento en cuestión.

La experiencia, en la vida real, nos dice que mientras más tiempo vive una persona, más fácil es de identificarla, atendiendo a como interactúa con otras personas. En el mundo virtual pasa lo mismo, mientras más se interactúa con otras personas u organismos, mayor facilidad tendrán para saber quién es a través de sus propios registros, que en muchos casos, en vez de identificar al individuo, forman un patrón de comportamiento o de conducta, que en multitud de situaciones vendrá de la confianza producida, en la exactitud de la información proporcionada por otra entidad o individuo a otra entidad, que realizó dicho registro a través de un pasaporte, DNI o NIF[372].

Desde este punto, es de donde se muestra y desde donde se puede crear la principal fortaleza del sistema, a través del propio registro en el sistema de identificación, pues con la validación o verificación de la identidad es posible combinar la información de una gran variedad de datos, que permite cotejar la información relativa a la identidad. Esta idea, cobra mayor virtualidad cuanto más nos acercándonos a un sistema de identidad federada, que han servido de guía a plataformas como STORK, en Europa, o SIFT[373], en la APEC.

[372] Nos referimos a la información que pueden proporcionar por ejemplo entidades como Equifax, Asnef, Experian, Badexcug, RAI, CIRBE o incluso el FIJ (Ficheros de Incidencias Judiciales).
[373] Véase, el Capítulo cuarto en referencia a la APEC (págs. 213 y ss.).

CAPÍTULO CUARTO: AUTENTICACIÓN/AUTORIZACIÓN DE LA TRANSACCIÓN

4.1. Introducción

Como hemos visto, la firma electrónica se compone de una función identificativa y una la función de autenticación de la identificación. La primera, la establecíamos como la designación de una persona de forma no ambigua, a través de un conjunto de datos que le son propios, mediante la emisión de una credencial, que le permitía saber a la persona decir quién es. La segunda, la establecíamos como un elemento intencional, que permitía a un sujeto vincularse al acto jurídico que se había creado; es decir, una verificación de que quien firma electrónicamente el documento es quien dice ser.

A estas dos funciones podemos sumarle una tercera, de autorización o de autenticación de la transacción, en el sentido que indica la Ley Modelo sobre Firma Electrónica, cuando nos indica que "…el firmante aprueba la información recogida en el mensaje de datos"[374]. De esta manera, una vez hecha la autenticación debida de una persona, la parte receptora debe realizar su propio proceso de autorización, para determinar los derechos y privilegios que se otorgan a esa persona. Este proceso plantea la pregunta: "¿a qué está usted autorizado?". Por ello, la autenticación de la identidad no constituye solamente un fin en sí.[375].

Este proceso se empleará, en muchos casos, para facilitar las decisiones de autorización de la parte receptora, de manera que, una vez autenticada la identidad de quien desee realizar la transacción electrónica, pueda utilizar un determinado método para autorizar y/o decidir, si procede a confirmar la realización de la transacción con el interesado o no, o, sin embargo, decide utilizar alguna otra forma la comunicación para proceder a la transacción.

---

[374] Artículo 2,a) *in fine* de la Ley Modelo sobre Firma Electrónica.

[375] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 9.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita: 26/3/2014).

4.2. Acercamiento a la pretendida neutralidad tecnológica

Esta función de autenticación o autorización se relaciona, necesariamente, con la transacción y, ésta, a su vez, con el método que se emplea para realizar la misma. La operación, como tal, resulta importante y entra de lleno en el contexto de la fiabilidad y/o seguridad y, además, probablemente más importante, la forma en que la identidad afecta a la autorización transacción. Solo de esta manera se puede entender mejor los problemas que se presentan en las operaciones transfronterizas y las medidas correctivas necesarias.

Si identificamos esta función como lo que realmente es: una forma de autorización de un servicio (autenticación de la identidad) y de una transacción (autenticación de la transacción), nos lleva a considerar la propia autorización, como un conjunto, que trata de contribuir al establecimiento de la fiabilidad y/o de la seguridad, como apoyo a la transacción.

Ante esta situación, nos encontramos como elementos a analizar, respecto de la transacción: la fiabilidad y/o la seguridad. Ambos deben ser tenidos en cuenta por razones evidentes: la fiabilidad nos lleva a unas prácticas de buen funcionamiento; o sea, nos da herramientas que nos llevan a detectar anomalías en las transacciones; la seguridad se dirige a una situación de protección efectiva, no a una transacción segura, porque es imposible, por mucho que nos empeñemos. Es por eso que, muchas veces, con el término seguridad lo que realmente se quiere decir es: confianza.

4.2.1. Fiabilidad

La fiabilidad como medio nos lleva a una probabilidad de buen funcionamiento. Desde el punto de vista de la transacción, cuando hablamos de fiabilidad, nos referimos a que un dispositivo trabaje correctamente durante un tiempo y en las condiciones en que se encuentre el servicio, de manera que quien una transacción tendrá que fijarse en los posibles riesgos.

Por consiguiente, identificamos la fiabilidad como un conocimiento del estado del sistema. Por ejemplo, iniciamos la contratación, en principio, desconocemos si tendrá éxito; pues, sólo una vez efectuada la transacción correspondiente se sabrá si existe o no fallo. Por otro lado, debemos decir que la fiabilidad no es una predicción, sino la probabilidad de actuación correcta del dispositivo de firma electrónica. Se trata, de que el dispositivo funcione bajo las condiciones fijadas, durante un periodo de tiempo determinado. Ante esto, se hace necesario determinar las funciones, funcionamiento, requisitos, etc.

Muchas veces, para aumentar la fiabilidad, se necesita reducir la complejidad del sistema, aumentar la fiabilidad de los componentes, que hacen posible la estampación de la firma, acoplan elementos redundantes o en reserva, revisan y prevén acciones preventivas etc. Por esta razón, pensamos que la fiabilidad se centra en las relaciones contractuales que puedan surgir entre quienes contratan electrónicamente, atendiendo a la libertad de las partes y, en virtud de lo dicho, las partes pueden convenir los efectos entre ellas, de un modo distinto al previsto en las leyes aplicables. Éstas quedan reducidas al valor de norma supletoria, cuya aplicación se producirá, únicamente en caso de que los contratantes hayan decidido su exclusión y sustitución por otras reglas distintas o de propia creación, más útiles a los fines perseguidos por ellas[376].

Hay excepciones potenciales, que se refieren principalmente a la confidencialidad de los datos electrónicos intercambiados con fines negóciales, dirigidas al régimen de responsabilidad, contraída por las partes; la libertad empresarial, en el establecimiento como prestador de servicios de certificación; o el reconocimiento nacional de firmas, certificadas los prestadores de servicios de certificación establecidos en diferentes Estados.

Fijémonos en aquellos Estados, que han recogido, en sus legislaciones, un criterio neutral, con respecto al uso de la firma electrónica: han prestado su atención en la fiabilidad y, con ella, en la intención; de tal manera que han excluido las excepciones potenciales a la libertad contractual de las partes. Por ejemplo, Estados Unidos considera que las firmas electrónicas son el equivalente funcional de las firmas

[376] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, págs. 61 y ss.

manuscritas, siempre que la tecnología empleada tenga la finalidad de desempeñar determinadas funciones específicas y cumpla, además, determinados requisitos de fiabilidad con respecto a la tecnología[377].

La legislación estadounidense establece, que la firma electrónica puede tomar múltiples formas, incluyendo sonidos electrónicos, símbolos o procesos. La única condición para que puedan ser calificadas como firma, es que deben presentar la intención de firmar el registro electrónico. Asimismo, a una firma no se negará efectos jurídicos, validez o fuerza obligatoria, por el hecho de estar en formato electrónico. Un contrato en relación con una transacción no se le negará efectos jurídicos, validez o fuerza obligatoria por el tipo de firma electrónica, que se utilizó para firmar; siendo las partes las que decidan, por sí mismas, si desea o no utilizar o aceptar una determinada firma electrónica

4.2.2. Seguridad y confianza

La seguridad se dirige a una situación de protección efectiva, para tratar de conseguir la confianza suficiente y para que las partes interactúen sin temor alguno[378]. Además de la confianza, con el uso del término seguridad se pretende dar a conocer dos caras de una misma moneda: una activa, para proporcionar un conjunto de mecanismos o prestaciones con el fin de evitar o prevenir accidentes; otra pasiva, para proporcionar un conjunto de medios que permitan proteger a las partes que intervienen en la transacción.

De esta manera, la seguridad, tal y como se plantea en muchas legislaciones y reglamentaciones, como medio, obvia la fiabilidad, apoderándose la seguridad de todo el protagonismo, pues lo que se pretende es ganar la confianza de las empresas, usuarios, consumidores, ciudadanos, etc. Esto es apreciable en numerosas legislaciones, que prescriben la tecnología como medio que nos lleva a la seguridad.

---

[377] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.83.
[378] RIBAS ALEJANDRO, J.: *Aspectos jurídicos del comercio electrónico en Internet,* Elcano, 2002, págs. 103 y ss.

Justamente, se habla siempre de políticas de seguridad[379]: reglas a las que tienen que atenerse quienes usan el sistema informático de una organización, para proteger tanto la información como la tecnología.

Las cuestiones de seguridad van evolucionando, en las distintas legislaciones, hacia el empleo de la firma digital, potenciando los efectos generadores de confianza, por el uso de la tecnología. Con el uso de la tecnología, se trata de generar confianza, especialmente de los ciudadanos, procurando crear una situación de tranquilidad pública, protección que se lleva a cabo por los entes públicos, que logran un *cuasi* monopolio, a la vez que un control de acceso en la materia, que no tiene justificación económica ni tecnológica.

Un claro ejemplo lo tenemos en la Unión Europea, que en la Directiva 1999/93/CE sobre firma electrónica y, posteriormente, en el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, que viene a sustituir la Directiva 1999/93/CE, pues, si bien recoge distintos tipo de firma electrónica, favorece el empleo de la firma digital.

En este nuevo marco normativo se observa mejor el intento de conseguir, a través de la seguridad, la confianza. Observemos el cambio terminológico que se produce, respecto a los prestadores de servicios de certificación, que pasan a denominarse proveedores de servicios de confianza.

La primera consideración que debemos hacer es el cambio de rumbo que se pretende con esta modificación. El término confianza es amplio y abstracto, ha sido analizado desde la psicología social, sociología, economía, marketing y literatura, sin que, hoy día, haya una definición unánime de qué debe entenderse por ella[380]. Sin embargo, tiende a utilizarse como una forma de referirse a las relaciones entre personas. Si uno confía en otro, el primero espera una buena conducta, una esperanza o, incluso,

[379] DORAL, A.: *Seguridad en Internet y medios de pago electrónicos*, Madrid, 2002, págs. 41 y ss.
[380] LÓPEZ JIMENEZ, D.: "Iniciativas empresariales de regulación del comercio electrónico: el supuesto de la península Ibérica", *Revista Electrónica de la Contratación*, núm. 114, 2011, págs.3 – 49.

una seguridad firme de que se va a hacer algo bien[381]. El término anteriormente usado, prestador de servicios de certificación, llevaba, tal vez, a inducir dependencia, en relación con el origen o la conexión de una sección de colectividad subordinada a un poder[382].

Si bien el proveedor de servicios de confianza y el prestador de servicios de certificación son lo mismo. Se pretende atraer la atención del usuario, creando un clima de confianza en un entorno determinado, necesario, por las características que tiene el marco en el que se desarrollan[383]. De esta forma, se quiere dar a entender como un proveedor de servicios, con sus acciones y sus caracteres, va conseguir, de Internet, un universo más o menos confiable para las personas, ya sean físicas o jurídicas.

4.3. La realidad tecnológica

4.3.1. El primer planteamiento internacional

Como sabemos, la necesidad de reconocimiento jurídico del uso de las nuevas tecnologías, a nivel internacional, llevó a la CNUDMI a aprobar las Leyes Modelo, sobre Comercio Electrónico y Firma Electrónica, con el fin de que sirviera a los Estados para que legislaran de una manera uniforme sobre estas materias.

A través de la Ley Modelo sobre Comercio Electrónico, la CNUDMI, en el Artículo 7, estableció un concepto de firma genérico y amplio, referido en relación con un mensaje de datos. Se optó por una posición de neutralidad respecto de la tecnología, al considerarse que optar por una concreta tecnología llevaba al riesgo de quedar obsoleta y la vigencia en el tiempo de la norma estaría en entre dicho, ya que no podría

[381] REAL ACADEMIA DE LA LENGUA ESPAÑOLA: *Diccionario de la lengua* española, Madrid, 2001.
Disponible en: http://www.rae.es/recursos/diccionarios/drae (última visita: 7/4/2014).
[382] JOS DUMORTIER, J.; VANEZANDE, N.: "Trust in the proposed EU regulation on trust services?" *Computer Law &Security Review*, Vol. 28, núm. 5, octubre, 2012, p. 568 -576.
[383] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final.

dar cobertura a futuros instrumentos técnicos cuyos usos pudieran ser implantarse en un futuro[384].

De este concepto, se infiere que se utilice un método para identificar a la persona y para indicar que ésta aprueba la información que figura en el mensaje de datos; de tal manera que, el método utilizado sea tan fiable como apropiado para los fines para los que se generó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente. El grado de fiabilidad se ha de determinar a la luz de los fines para los que se genera la información, tratándose de nuevas tecnologías estas pueden ser de diversa índole[385].

Con la Ley Modelo sobre Firma Electrónica se define la firma electrónica en su Artículo 2,a) como "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos".

Esta definición recogida es más acotada[386] que el concepto subyacente en el Artículo 7 de la Ley Modelo sobre Comercio Electrónico. Con ella, se pretende que ésta sea lo suficientemente amplia como para abarcar las firmas electrónicas existentes en la actualidad y las que puedan utilizarse en el futuro, con independencia de la tecnología o métodos empleados, en equivalencia con las firmas manuscritas. No obstante, es necesario hacer una precisión, la Ley Modelo sobre Firma Electrónica pretende ser neutral tecnológicamente, no lo es totalmente; pues la reconducción que se efectúa, hacia esta neutralidad, es más un deseo que una realidad, ya que: se utilizan conceptos, por ejemplo, el de certificado, que sólo tienen sentido en la medida en que se utilizan en una infraestructura de clave pública, siguiendo un estructura triangular típica de esta

[384] MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de la Contratación Electrónica*, núm. 15, Abril, 2001, págs. 3 - 60.
[385] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 184.
[386] MADRID PARRA, A*:* "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista de Derecho Patrimonial,* año 2003 – 2, número 11, págs. 31 – 63.

infraestructura; al regular el proceder del firmante, el prestador de servicios de certificación y el tercero que confía[387].

La Ley Modelo sobre Firma Electrónica[388]: traza una distinción entre la noción de "firma" y la noción técnica de "firma electrónica", término especializado que comprende algunas prácticas que no intervienen, necesariamente, en la producción de firmas jurídicamente pertinentes. En la preparación de la Ley Modelo[389] ya se estimó, que había que señalar la atención de los usuarios ante el riesgo de confusión, que podría resultar el uso del mismo instrumento técnico, para la producción de una firma jurídicamente pertinente y para otras funciones de autenticación o identificación.

De esta forma, se llama la atención de que las técnicas de firma electrónica pueden servir para otros fines, además, de las funciones consideradas básicas para las firmas tradicionales, como puede ser identificar al emisor de un mensaje, sin mostrar su aprobación sobre el mismo, en cuyo caso, según la CNUDMI, no se buscará la equivalencia funcional con las firma tradicionales. Con esta advertencia, se están recogiendo los límites propios del principio de equivalencia funcional[390], considerando a la firma electrónica, como un medio eficaz para identificar a una persona y dar fiabilidad a la información insertada en un mensaje de datos[391].

Con el Artículo 6 de la Ley Modelo sobre Firma Electrónica, Artículo de gran importancia, que sigue la pauta marcada en el Artículo 7 de la Ley Modelo de Comercio Electrónico, el cual regula, con carácter general, sin entrar en especificaciones en el concreto uso, las funciones de la firma: identificación de la persona, certificación de la participación de la persona en el acto en concreto y la vinculación de esa persona con el documento en sí[392]. Además, regula las funciones de fiabilidad. Todo ello con un único

---

[387] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 208.
[388] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE*, párr. 94 y ss.
[389] CNUDMI/UNCITRAL: *A/CN. 9/ 483 - Informe del grupo de trabajo sobre comercio electrónico acerca de la labor de su 37º período de sesiones*, Viena, 6 de octubre de 2000, párr. 62.
[390] CRUZ RIVERO, D.: "Análisis del concepto de firma electrónica como equivalente de la firma manuscrita", *Revista de la Contratación Electrónica*, núm. 60, mayo, 2005, pág. 3 – 122.
[391] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE*, párr. 63.
[392] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma electrónica y autoridades de certificación*, Madrid, 2000, pág. 39.

propósito: asegurar que la firma electrónica tenga idénticas consecuencias jurídicas que la firma manuscrita y cumplir el requisito del documento escrito y formato original, exigido en muchos Estados.

Hay que resaltar dos aspectos importantes: primero, la fiabilidad técnica, que otorgará la autoridad certificadora, al ser esencial para la Ley Modelo que cumpla con el objetivo de dar certeza a la Ley Modelo sobre Comercio Electrónico, en cuanto a los efectos jurídicos que cabe esperar[393]; segundo, el interés básico de la firma electrónica, de cara su empleo como prueba, radica en la certeza, en su presencia con determinadas garantías, que determine su valor probatorio[394].

Ante esto, el párrafo 3 del Artículo 6 establece una serie de requisitos, que si se cumplen, se presume la fiabilidad del método utilizado y, por ello, la firma electrónica surte efectos jurídicos. De esta manera, en la medida en que, la firma electrónica se configura como instrumento, permite satisfacer tales exigencias, como equivalente de la firma manuscrita, y puede contribuir a superar, plenamente, para las transacciones en Internet, las dificultades inherentes a la ausencia, en este contexto, de firma manuscrita, cumpliendo las funciones básicas de ésta en el ámbito contractual, que son constituir un signo de identificación personal y representar la voluntad de obligarse[395].

El conjunto de lo dicho en el Artículo 6 de la Ley Modelo sobre Firma Electrónica se complementa con lo establecido para el "proceder del firmante" (Artículo 8), el "proceder del prestador de servicios de certificación" (Artículo 9 y 10) y el "proceder de la parte que confía en el certificados" (Artículo 11), siendo lo que nos interesa, en este momento, los Artículos 9 y 10.

El Artículo 9 recoge el "proceder del prestador de servicios". Éste recoge su sometimiento a unos principios que determinaran su responsabilidad, dejando en manos del derecho nacional la determinación de las consecuencias jurídicas de su incumplimiento, al igual que lo hace con el firmante en el párrafo segundo del Artículo 8 de la Ley Modelo. El establecimiento de mecanismos de seguridad y autenticación

[393] MADRID PARRA, A: Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas". *Revista Derecho Patrimonial*, año 2003 – 2, núm. 11, págs. 31- 63.
[394] DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 401.
[395] DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 389.

requiere la intervención imprescindible de los prestadores de servicios; siendo necesaria para garantizar la asociación de todas las partes que entran en juego[396].

El proceder del prestador de servicios de certificación se estructura en torno a la emisión y contenido del certificado. Cuando existe, en relación con la firma electrónica, es porque ésta se basa en la infraestructura de clave pública. Ante esta situación, se apunta el epígrafe "realidad tecnológica"; pues la CNUDMI tuvo presente desde un inicio la existencia predominante, en su momento, de la infraestructura de clave pública, disponiendo que cuando la firma electrónica reúna especiales requisitos, que son los propios de las firmas electrónicas digitales, gozará, a su favor, de una presunción de validez jurídica[397].

En nuestra opinión, se hizo lo correcto. Proporcionó un punto de referencia a todos los Estados, sobre cómo realizar una legislación acorde a las necesidades vigentes y futuras; asimismo, dio una información adicional, acerca del reconocimiento de la firma electrónica y certificados extranjeros, y respecto de la legislación de otro país, determinando efectos de la firma electrónica, con tecnología digital o sin ella, y definiendo la responsabilidad de todas las partes, que pueden llegar a participar en una transacción.

Tras las comentadas Leyes Modelos, la CNUDMI adoptó la Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales que, como sabemos, se basa en la Ley Modelo sobre Comercio Electrónico y en la Ley Modelo sobre Firma Electrónica, considerándose estos textos, como las pautas a seguir al establecerse en la Convención los mismos principios fundamentales, fijados en las Leyes Modelos, tales como: la neutralidad tecnológica y la equivalencia funcional. Aunque, también, entran en juego otros como: la autonomía de la voluntad, la libertad de forma y la inalterabilidad del Derecho preexistente[398].

---

[396] DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 407.

[397] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", *en Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 208.

[398] OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, págs. 45-88.

Se quiere, con esto, que los principios y reglas generales contenidos en las Leyes Modelos pasen a un cuerpo normativo jurídico internacional, que tenga naturaleza de Derecho objetivo directamente aplicable, dándose un nuevo impulso al uso de las nuevas tecnologías, en la contratación relacionada con el comercio internacional[399].

Con la neutralidad tecnológica[400], se trata de no depender de la utilización de determinados tipos de tecnologías, que puedan aplicarse a la comunicación y al archivo de cualquier tipo de información. La neutralidad tecnológica es importante para favorecer los avances tecnológicos, dándoles cabida en un futuro y, al mismo tiempo, tratar de evitar que las normas caigan en desuso. Por ello, la Convención evita toda referencia a medios técnicos concretos de transmisión o archivo de información.

Por otro lado, la neutralidad tecnológica también hace referencia a la neutralidad de los medios; pues la Convención se ha concebido de manera que se faciliten los medios de comunicación sin papel, previniendo criterios para que esos medios puedan equipararse a documentos sobre papel. En la neutralidad de los medios, se plantean cuestiones como la seguridad debida al riesgo existente en las comunicaciones.

Con respecto al principio de equivalencia funcional[401], se basa en tres elementos identificables "escrito", "firma" y original", debiendo ampliarse sus conceptos con miras a abarcar las técnicas informáticas en su ámbito.

Para analizar estos conceptos, en los que se basa este principio de equivalencia funcional, debemos irnos a un Artículo esencial de la Convención, al Artículo 9 que tiene por enunciado "Requisitos de forma", donde trata estos conceptos de forma separada, con el fin de evitar cualquier posibilidad de solapamiento entre ellos. En su apartado segundo, recoge el elemento "escrito" conforme a lo previsto en el Artículo 6

[399] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 229.

[400] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 47.

[401] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 50.

de la Ley Modelo sobre Comercio Electrónico, dándose relevancia no al soporte, sino a la información que ha de quedar garantizada en cualquier caso.

Como hemos dicho al hablar de la identificación, la Convención, ante la utilización de técnicas electrónicas de autenticación, en lugar de las firmas manuscritas y otros procedimientos tradicionales de autenticación, ha creado la necesidad de establecer un marco jurídico específico, que reduzca la incertidumbre sobre los efectos jurídicos, que puedan derivar de la utilización de esas técnicas modernas, que la Convención denomina como "firmas electrónicas".

La Convención trata de asegurar el nexo entre el firmante y la información[402]. Con ello, además de identificar, trata de indicar la intención de éste, con respecto a la información consignada en la comunicación electrónica; de tal manera que, de forma que el método empleado, para la identificación, pueda ser tan fiable como apropiado para los fines para los que se generó la comunicación. Se pone de relieve la importancia de la integridad de la información, para que mantenga su carácter original, y enuncia los criterios a tener en cuenta para evaluar la integridad, refiriéndose al registro sistemático de la información, a la garantía de que la información ha sido registrada sin lagunas y a que se hayan protegido los datos frente a toda alteración. Estableciéndose un vínculo entre originalidad y autenticación[403].

4.3.2. Enfoques tecnológicos encontrados tras la pretendida neutralidad tecnológica

Como hemos visto, la Ley Modelo sobre Firma Electrónica establece, de partida, un planteamiento tecnológicamente neutral, aunque su estructura y contenido nos está describiendo el esquema de la infraestructura de clave pública, basada en la criptografía asimétrica, que utiliza una clave privada y otra pública. No obstante, en una visión de

[402] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 245.
[403] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 169.

conjunto, se puede concluir, que recoge la posibilidad neutral, la tecnología presente y la innovación futura.

Tras la Ley Modelo han sido muchas las distintas legislaciones y reglamentaciones que se han adoptado sobre la autenticación electrónica, que reflejan distintos supuesto sobre la firma electrónica y su condición jurídica.

Precisamente, con la mirada puesta en el enfoque neutral y el mencionado esquema marcado por la CNUDMI, en la referida Ley Modelo, se pueden señalar tres enfoques principales, para abordar las tecnologías de firmas y autenticación electrónica: enfoque minimalista, enfoque de tecnología específica y enfoque de doble nivel.

4.3.2.1. Enfoque minimalista

Se trata de un enfoque legislativo diseñado para ser completamente neutral tecnológicamente y, por tanto, no dar trato preferencial a ninguna tecnología sobre las demás existentes. Asimismo, las partes pueden elegir la tecnología que, según su criterio, consideren más oportuna o que más garantías dé para realizar la transacción.

Este enfoque otorga, al mercado, la facultad de determinar qué tecnología es la más favorable por tres razones: a) el exceso de regulación puede impedir el desarrollo natural del mercado; b) una regulación específica de la tecnología, ahogaría una posible innovación tecnológica; c) la legislación que regula, exclusivamente, una tecnología determinada podría frenar las transacciones internacionales y la uniformidad reglamentaria en todo el mundo[404].

Por consiguiente, algunos Estados, que han adoptado este enfoque legislativo, se limitan a afirmar, sin más, que a la firma electrónica no se les debe negar validez legal o fuerza obligatoria, por el hecho de estar en forma electrónica; pues, consideran que el establecimiento de requisitos relativos a la certificación en una jurisdicción puede suponer una carga para otros, en cuya jurisdicción no podrá exigir dicho certificado

[404] MIYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *ScienceDirect Rreview*, enero, 2007, pág.49.

4.3.2.1.1. Estados Unidos

Un ejemplo de enfoque minimalista es la legislación establecida en Estados Unidos, que ha "solidificado" el marco legal, para el uso de los documentos electrónicos y firmas electrónicas, en el comercio electrónico, con la aprobación de la *Uniform Electronic Transactions Act* (UETA), en 1999, (Ley que ha sido promulgada en la mayoría de los Estados) y la *Electronic Signatures in Global and National Commerce Act* (E-Sign), en el 2000.

La E-Sign está diseñada para completar la UETA, que a su vez ha sido adoptada por muchos Estados de la Unión. La E-Sign da un marco regulatorio a aquellos Estados que no han adoptado la UETA. Ambas están influida por las Leyes Modelo de la CNUDMI, adoptando un enfoque minimalista, que busca evitar cualquier discriminación manifiesta, que suponga favorecer una tecnología concreta; es decir, son neutrales tecnológicamente, o lo que es lo mismo, no dan tratamientos presuntivos favorables a la utilización de una tecnología, o una categoría tecnológica. Por ello, cualquier tecnología tiene un tratamiento jurídico similar[405].

Según el criterio minimalista, se considera que las firmas electrónicas son el equivalente funcional de las firmas manuscritas, siempre que la tecnología empleada tenga la finalidad de desempeñar determinadas funciones específicas y cumplan, además, determinados requisitos de fiabilidad, con respecto a la tecnología[406]. Estas funciones son las de identificar al firmante e indicar la intención de éste respecto de la información firmada.

Este enfoque ofrece una posibilidad mayor de obtener una legislación uniforme, sobre la firma electrónica, basándose en criterios armonizados internacionalmente, ya que se centra más en las funciones propias de la firma electrónica que en los métodos o

[405] MIYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *ScienceDirect Rreview*, enero 2007, pág. 49.
[406] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.83.

aplicaciones tecnológicas en que éstas puedan traducirse; manteniendo una postura de perfil neutral[407].

El objetivo es el uso uniforme, el reconocimiento y la ejecución de la firma electrónica y los e-registros, a través de la eliminación de obstáculos legales existentes en el comercio en línea, estableciendo un estatuto de neutralidad. Lo cual se plasma con nitidez en el Código de los Estados Unidos donde se establece, entre otros principios, la eliminación de los obstáculos a las transacciones electrónicas, mediante la adopción de los principios pertinentes de la Ley Modelo sobre Comercio Electrónico, aprobada en 1996 por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional.

La Ley Modelo sobre Comercio Electrónico se ocupa de las funciones de la firma electrónica y su poder vinculante, a la vez que reconoce, en los mismos términos que en el Código de los Estados Unidos, la adopción de enfoques no discriminatorios a las firmas electrónicas y métodos de autenticación. De esta forma, establece una serie de principios que no tienen otra función, más que, la de fomentar la confianza en la información y las comunicaciones, para facilitar el comercio electrónico internacional[408].

Así, las leyes americanas adoptan parámetros de equivalencia funcional, respecto a cualquier transacción, nacional o internacional, estableciendo que una firma electrónica, contrato u otro documento electrónico, no se le negará efectos jurídicos ni validez legal, por el mero hecho de estar en formato electrónico. Asimismo, a un contrato electrónico no se le puede negar efectos jurídicos, validez o fuerza obligatoria, únicamente, por la firma electrónica o registro electrónico utilizado.

De esta manera, se considera la firma electrónica como el medio idóneo para sustituir a la firma tradicional, resultando irrelevante la tecnología empleada para firmar el mensaje, lo que da estabilidad al ordenamiento jurídico ante los continuos avances técnicos. Sin embargo, en nuestra opinión, la defensa a ultranza de este principio podría

[407] SPYRELLI, C.: "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", *Journal of Information, Technology and Law*, vol. 2002, núm. 2, 2002, pág. 3 – 59.

[408] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005 pág. 10 y ss.

suponer una reducción de los requisitos de firma electrónica, a pesar de tener un nivel de seguridad aceptable.

A lo que se ha dado respuesta a través del concepto de firma electrónica en la E-Sign y en la UETA, que han adoptado una firma electrónica verdaderamente equivalente a la firma manuscrita; pues, separa los lastres conceptuales adheridos a la firma electrónica como consecuencia de la evolución histórica de la institución y de esta forma, describe la firma electrónica como "un sonido electrónico, símbolo o proceso, unido o asociado lógicamente a un contrato o a otro documento y ejecutado o adoptado por una persona con la intención de firmar el registro". Esto podría decirse que es una definición ejemplificativa y simple, pero delimita, perfectamente, la firma electrónica, como lo que debe ser, una firma en forma, no manuscrita, sino electrónica[409].

Al mismo tiempo, llama la atención la flexibilidad; pues, lo ideal es que el uso de la firma electrónica sea posible en una gran variedad de circunstancias. Por ello, evoca no sólo una semejanza en cuanto a su función o incluso a su fuerza probatoria, respecto de la identidad del firmante, sino ante todo, un deseo de que el nuevo instrumento electrónico sea considerado firma a efectos de cumplir los requisitos formales[410]; de este modo, la firma electrónica es un elemento constitutivo del escrito, capaz de garantizar la integridad e inalterabilidad del documento; pues, la utilización de los medios electrónicos de comunicación no implican una alteración de los requisitos y efectos de las declaraciones jurídicas, sino que allí donde sea necesario y posible, las exigencias formales previstas en el ordenamiento, deberán cumplimentarse mediante equivalentes electrónicos.

Así pues, se permite, a los proveedores de bienes y servicios, a que puedan seleccionar la firma electrónica más aceptable y eficaz para el producto en línea que ofrezcan, de tal manera que podrán optar desde un simple "clic", a un número "PIN", a un código numérico cifrado, a datos biométricos e, incluso, una imagen digitalizada de una firma manuscrita. Así pues, no solo se reconoce la firma digital, sino que también se permite el uso de cualquier tipo de tecnología, con el fin de facilitar la contratación en línea.

[409] CRUZ RIVERO, D.: *Eficacia formal y probatoria de la firma electrónica*, Madrid, 2006, pág. 22.
[410] CRUZ RIVERO, D.: *Eficacia formal y probatoria de la firma electrónica*, Madrid, 2006, pág. 27.

El Departamento de Comercio, en un informe remitido al congreso de los Estados Unidos de América[411], en una clara referencia a la tecnología PKI, reconoce que la tecnología puede proporcionar una solución al uso de las firmas electrónicas, en muchos de los complejos problemas que se relacionan en el comercio electrónico, ofreciendo elementos de seguridad. Sin embargo, las Leyes no deben prescribir una tecnología en particular, sino que deben dejar esas opciones al mercado, permitiendo la creación y aplicación de tecnologías, para proporcionar eficacia y seguridad al comercio, de manera que puedan conllevar a una proliferación de mecanismos, que compitan por llevar a cabo un mayor uso de los medios electrónicos.

Se establece el uso voluntario de firmas electrónicas a través de sistemas de consentimiento expreso, para que los consumidores, por un lado, puedan elegir cualquier forma de transacción (autonomía de la voluntad) y, por otro, si se ponen de acuerdo, puedan realizar transacciones en línea que afirmen su intención por vía electrónica[412]**.**

Incluso las Leyes van más allá, al establecer que la empresa deberá proporcionar al consumidor una información clara y visible antes de dar su consentimiento, tales como: informar de cualquier derecho u opción a tener el registro en una forma no electrónica, describir los procedimientos que tiene el consumidor para retirar el consentimiento, estar provisto de los requisitos de hardware y de software para el acceso y retención de documentos electrónicos, etc.[413].

Por otro lado, la firma electrónica, como hemos dicho, requiere "intención". Sin embargo, nada se dice sobre la forma de establecer la intención, lo que deja la firma, respecto a la forma de atribuirla a una persona y a sus consecuencias legales, a lo que se diga en otras leyes y a las circunstancias de hecho que la rodeen, lo que crea incertidumbre. Si la autenticidad de una firma está en disputa, la persona que busca

[411]DEPARTMENT OF COMMERCE; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (USA): Report *to Congress: Electronic Signature in Global National Act. Section 105 (a)*, junio de 2001.
Disponible en: http://www.ntia.doc.gov/files/ntia/publications/105areport.pdf (última visita: 3/5/2014).
[412] SPYRELLI, C.: "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", *Journal of Information, Technology and Law*, vol. 2002, núm. 2, 2002, pág. 3 – 59.
[413] E-Sign: Section 101.

hacerla cumplir, estará obligada a demostrar que la firma fue ejecutada por la persona que la hubiere solicitado; lo que significa que las partes que aceptan la firma electrónica tendrán que estar convencidas, de que la firma es suficientemente verificable, dadas las circunstancias previstas para contrarrestar el riesgo de este tipo de conflictos[414]. Lo que es fiel reflejo, de que el lugar de origen, no debe ser en modo alguno, *per se*, un factor determinante al decidir si los certificados o las firmas electrónicas, de origen extranjero, deben ser susceptibles, o no, de surtir efectos jurídicos, o en qué medida los producen. De esta forma, la determinación de si un certificado o firma electrónica es susceptible de eficacia jurídica debe depender de su fiabilidad técnica y no del lugar en que se expedida[415].

Con ello, se pretende promover la aceptación y uso de firmas electrónicas en el ámbito internacional[416]. Para lograr este objetivo, se observa la falta de disposiciones detalladas en relación con el reconocimiento de servicios de certificación, o acerca de certificados emitidos por proveedores de certificación establecidos en el extranjero[417]. La disposiciones existentes, son de carácter no discriminatorio, similares a las del Artículo 12 de la Ley Modelo sobre Firma Electrónica, que estipulan que el lugar de origen *per se*, no debe ser un factor para determinar si, los certificados o firmas

[414] Disponible en: http://www.idmanagement.gov/documents/Use_of_ESignatures_in_Federal_Agency_Transactions_v20_20130125.pdf (última visita: 12/5/2014).

[415] Artículo 7031 apartado (a), Capítulo 96, Título 15 del Código de los Estados Unidos nos dice textualmente:
"(a) Promotion of electronic signatures: (1) Required actions: The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 7001 of this title. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce; (2) Principles: The principles specified in this paragraph are the following: (A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law; (B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced; (C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid; (D) Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions."

[416] Sec 301 (a) (1) of Electronic Signature in Global and National Commerce Act.

[417] MIYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *ScienceDirect Rreview*, enero 2007, pág. 42.

electrónicas extranjeras, deben reconocerse como susceptibles de eficacia jurídica en un Estado promulgante[418].

4.3.2.1.2. Australia

Otro ejemplo de enfoque minimalista lo tenemos en Australia, que a través de su *Electronic Transactions Act* (1999) ha adoptado una política de neutralidad tecnológica, en el reconocimiento de todas las tecnologías de firma electrónica, otorgando una condición jurídica mínima a todas las formas de firma electrónica. La Ley no dice lo que debe entenderse por firma electrónica, no lo hace ni a través del tradicional Artículo referente a definiciones. De esta forma, la intención de la Ley es establecer la firma electrónica como un medio necesario, para permitir a una persona satisfacer el requisito legal de firma manuscrita, mediante el uso de una comunicación electrónica, que contiene un método que identifica a la persona y que indica la aprobación de la información comunicada, en el sentido indicado en la Ley Modelo sobre Comercio Electrónico.

Como sabemos, las Leyes Modelo de la CNUDMI representan un conjunto, internacionalmente aceptado, de normas relativas al comercio electrónico, ejerciendo una influencia mundial en todos los ordenamientos jurídicos. Australia, no fue una excepción, lo mostró de manera clara en la redacción de su Artículo 10[419], antes de su modificación, en su apartado primero, nos decía: si, en virtud de una Ley de la

[418] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 159 (En relación con los principios que rigen la utilización de las Firmas Electrónicas en las operaciones internacionales en la E-Sign).

[419] ELECTRONIC TRANSACTIONS ACT (1999):
"10. Signature Requirement for signature:
(1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if: (a) in all cases--a method is used to identify the person and to indicate the person's approval of the information communicated; and (b) in all cases--having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and (c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements--the entity's requirement has been met; and (d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity--the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a)".

Commonwealth, se requiere la firma de una persona, este requisito quedará satisfecho en relación con una comunicación electrónica: a) en todos los casos, si el método se utiliza para identificar a la persona y para indicar la aprobación de la información comunicada de ésta persona; b) en todos los casos, si teniendo en cuenta todas las circunstancias pertinentes, en el momento en que se utiliza el método anterior, éste es tan fiable como apropiado, para los fines para los generó el comunicado o la información; c) que la persona, a la que se requiere la firma, debe dar su consentimiento a la exigencia del método usado, que debe ser conocido según lo contemplado en el apartado a). En este punto, resulta importante reseñar como en el caso Faulks v Cameron, en el cual el Tribunal se mostró convencido de que la firma impresa en los e-mails de la parte demandada: identificaba e indicaba su aprobación respecto de la información comunicada, que el método era tan fiable como apropiado y que el demandante dio su consentimiento al método utilizado, por lo que aplicando los requisitos mencionados, daba validez a la firma[420].

El requerimiento de firma, se resume en: si la aparente aprobación va a depender de la eficacia y fiabilidad, para que se produzca una vinculación; es decir, del método utilizado para la identificación del firmante y en la indicación de que el firmante aprueba la información expresada en el mensaje, todo va a girar en torno al significado de identidad, en el sentido de que identificar a una persona cualquiera, implicará un proceso de adecuación de la prueba, que se presentará con los hechos conocidos con anterioridad, momento en el que se va a confiar en la determinación de la persona con la que se va a contratar. Así pues, la fiabilidad de todo el proceso dependerá de la extensión y la confiabilidad de la prueba, que se presenta en la actualidad; el alcance y la fiabilidad de los hechos conocidos con anterioridad y la precisión de la coincidencia

[420] Faulks v Cameron [2004] NTSC 61:
"[63] The agreement is not signed in handwriting. It is unnecessary to refer to the many cases about electronic or telexed signatures such as, for example, Torrac Investments Pty Ltd v Australian National Airline Commission (1985) ANZ Conv R 82 where Derrington J held a telex authenticated with a printed name was signed. Section 9 of the Electronic Transactions Act provides: (1) If, under a law of the Territory, the signature of a person is required, the requirement is taken to have been met in relation to an electronic communication if – (a) a method is used to identify the person and to indicate the person's approval of the information communicated; (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and (c) the person to whom the signature is required to be given consents to the requirement being met by the use of the method referred to in paragraph (a).
[64] I am satisfied that the printed signature on the defendant's e-mails identifies him and indicates his approval of the information communicated, that the method was as reliable as was appropriate and that the plaintiff consented to the method".

entre los dos, en un contexto electrónico, que podría incluir la fiabilidad del medio a través del cual se lleva a cabo el mensaje. Este proceso es propio de los enfoques neutrales, desde el punto de vista tecnológico, en especial, los que, incluyen una "prueba de fiabilidad"[421] tienden a resolver las incompatibilidades legales.

De lo anterior, se puede observar cómo se adoptó el Artículo 7 de la Ley Modelo sobre Comercio Electrónico[422], refiriéndose de forma clara a las dos funciones principales de las firmas manuscritas; es decir, identificar al firmante e indicar la intención de éste respecto de la información firmada. No hay exigencias tecnológicas, centrando toda la atención en el método usado, para comunicar la aprobación de la intención y para asegurar que ésta debe ser apropiada para el propósito en que se realiza la comunicación; o sea, lo importante es la forma en que se aprueba la intención manifestada y el método apropiado para esa transacción en particular.

Sin embargo, observamos un añadido en la Ley australiana respecto al Artículo 7 de la Ley Modelo, en referencia a: las circunstancias pertinentes en el momento en que se utiliza el método (Artículo 10, b - ab initio). Esto permite una determinación de validez de un método de firma, incluso donde los avances en la tecnología han sido poco fiables, siempre y cuando, en el momento del uso, era un método fiable. Las disposiciones australianas también incluyen el requisito adicional del consentimiento de la persona a quien se le requiere la firma, que viene dado por la aprobación, no por la intención sin más. El problema se deriva de que no se introdujo ninguna distinción, entre la situación en que, los usuarios del comercio electrónico, están vinculados por un acuerdo de comunicaciones y la situación, en que las partes no tengan ninguna relación contractual previa, relativa al empleo del comercio electrónico[423]. Nos referimos a la incertidumbre creada, acerca de la suposición de cuando una firma se utiliza, para estar de acuerdo o para aprobar el contenido del mensaje.

De esta forma, al igual que el Artículo 7 de la Ley Modelo sobre Comercio Electrónico establece una norma mínima de autenticación, para los mensajes de datos

[421] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas*, Viena, 2009, párr.170.
[422] MASON, S.: *Electronic Signature in Law*, Cambridge, 2011, pág.158 y ss.
[423] FORDER: J.: "The inadequate legislative response to e-signatures", *Computer Law &Security Review*, vol. 26, núm.4, julio, 2010,págs.418-426.

intercambiados en ausencia de una relación contractual previa y, al mismo tiempo, da orientación sobre lo que, eventualmente, podría suplir la firma cuando las partes recurrieran a comunicaciones electrónicas en el contexto de un convenio de comunicaciones. Su finalidad era la de aportar una orientación útil, cuando el derecho interno deje totalmente a la discreción de las partes la cuestión de la autenticación de los mensajes de datos y, en un contexto, en que los requisitos de firma, normalmente fijados por disposiciones imperativas de derecho interno[424], son impuestos por Leyes de los Estados y territorios de un país federado, como es Australia[425]. Esta cuestión se considera en relación con el escenario legislativo mundial, puede presentar dificultades con cada uno de los requisitos para realizar una firma válida[426].

Ante los problemas planteados, en tanto que "lo ideal sería desarrollar régimen general de las transacciones electrónicas, con el fin de evitar una dualidad de regímenes para los contratos internacionales y nacionales"[427], la Ley fue modificada en 2011. Esta modificación comenzó el 10 de noviembre de 2008, cuando el Gobierno de Australia, en consulta[428] con los Estados y territorios, comenzó a considerar si Australia debería adherirse a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005. Finalmente, se optó por incorporar determinadas disposiciones sustantivas de esta Convención[429]. Entre

[424] CNUDMI/UNCITRAL: *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, 1999, párr.58 y ss.

[425] Todos los Estados y territorios de Australia (al igual que ha pasado en Estados Unidos) han aprobado Leyes paralelas: Electronic Transaction Act de 2000 (Nueva Gales del Sur); Electronic Transactions de 2000 (Queensland); Electronic Transactions Act de 2000 (Australia Meridional); Electronic Transactions Act de 2000 (Tasmania); Electronic Transactions de 2000 (Victoria); Electronic Transactions Act de 2003 (Australia Occidental); Electronic Transactions Act de 2001 (Territorio de la Capital Australiana); Electronic Transactionsde 2000 (Territorio del Norte). Si observamos los países donde se ha optado por las en sus ordenamientos jurídicos Leyes Modelo sobre Comercio Electrónico y Firma Electrónica, con referencia a todos sus principios, especialmente, la equivalencia funcional y la neutralidad tecnológica, son Estados con organización federal.

[426] FORDER: J.: "The inadequate legislative response to e-signatures", Computer Law &Security Review, vol. 26, núm.4, julio, 2010,págs.418-426.

[427] ATTORNEY-GENERAL'S DEPARTMENT: *Australia's accession to the UN Convention on the Use of Electronic Communications in International Contracts 2005: Proposed amendments to Australia's electronic transactions laws (consultation paper)*, noviembre 2008.
Disponible en:
http://www.ag.gov.au/Consultations/Documents/AustralianecommercereviewUNConventiononElectronicCommunications/UN%20Convention%20on%20ecommerce.pdf (última visita: 6/6/2014).

[428] ATTORNEY-GENERAL'S DEPARTMENT: *Australian e-commerce review - UN Convention on Electronic Communications (Consultation Process)*.
Disponible en:
http://www.ag.gov.au/consultations/pages/AustralianecommercereviewUNConventiononElectronicCommunications.aspx (última visita: 6/6/2014).

[429] Situación actual Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).

ellas se encuentra el Artículo 9, intitulado “los requisitos de forma”, en referencia al requerimiento de firma.

De este modo, la *Electronic Transactions Acts*, en su Artículo 10, cuando requiere una firma electrónica, está será válida: si, cuando la ley de algún Estado de la Commonwealth, requiera que una comunicación o un contrato sea firmado por una parte, este requisito que se considera cumplido en relación con una comunicación electrónica: a) en todos los casos, si se utiliza un método para identificar a la persona y para indicar la intención de esa persona en relación con la información comunicada; b) en todos los casos, si el método utilizado fue: i) tan fiable como sea apropiado para los fines para los que se generó o comunicó, a la luz de todas las circunstancias, incluyendo cualquier acuerdo aplicable a la comunicación electrónica; o ii) se ha demostrado, de hecho, que se han cumplido las funciones enunciadas en el apartado a), por sí sola o junto con una prueba más.

Respecto de la anterior regulación, se mantienen principios establecidos con anterioridad: equivalencia funcional y neutralidad tecnológica; pues, se sigue un criterio flexible de equivalencia funcional, entre las firmas electrónicas y las firmas sobre papel, y sigue sin establecer equivalentes tecnológicos a las funciones específicas de las firmas manuscritas, en el mismo, tal y como están previstos en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales. Sin embargo, si se aprecia un cambio terminológico: la "aprobación" por parte del firmante de la información, se sustituye por la “intención” de la persona respecto de la información comunicada.

Asimismo, se hace un añade un nuevo párrafo, el apartado ii-b), con el que se trata de fijar la cuestión problemática anterior (en relación con cuando una firma se utiliza para estar de acuerdo o aprobar el contenido del mensaje) evitando que una parte, en una operación en la que se requiera una firma trate de eludir sus obligaciones, negando que su firma sea válida, no por considerar que el presunto firmante no firmó, o que el documento firmado ha sido alterado, sino por estimar que el método de firma empleado

---

Disponible en: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model_status.html (última visita: 6/6/2014).

no es "tan fiable como apropiado" en las circunstancias del caso. Así, se viene a decir que, si la falta de fiabilidad potencial del método de firma no llegó a causar un problema en los hechos, el método de firma se debe tratar como fiable. Por ello, validaría el método de firma en cuestión, sin tener en cuenta su fiabilidad objetiva[430], siempre que el método utilizado demuestra, de hecho, que identifica al firmante e indica la intención del con respecto a la información contenida en la comunicación electrónica.

Este cambio legislativo, siguiendo la Convención, en pro de la facilitar aún más las pruebas de fiabilidad, da a la Ley un planteamiento que facilita, en la práctica, la utilización transfronteriza de la firma electrónica y su autenticación; pues, con arreglo al mismo es posible usar, válidamente, cualquier método de firma o autenticación electrónica, para firmar o autenticar un contrato o comunicación, siempre que satisfaga las anteriores condiciones generales. Sin embargo, la consecuencia de este enfoque es que, por lo general, esas condiciones se confirman solamente a posteriori y no hay ninguna garantía de que un tribunal reconozca la utilización de un método determinado[431].

4.3.2.2. Enfoque de tecnología específica

Frente al enfoque minimalista surge el enfoque de tecnología específica. Se trata de un enfoque prescriptivo, que se centra, exclusivamente, en el establecimiento de un marco jurídico único, a favor de una firma electrónica, basada en una tecnología concreta, generalmente, la tecnología PKI sobre la que se basan las firmas digitales. Son ejemplos característicos de la adopción de este enfoque la CCI, la ABA, la APEC o MERCOSUR.

Este enfoque surge, frente al anterior, al considerar que algunos tipos de firma electrónica pueden dañar la protección de las partes que intervienen en una transacción,

---

[430] ATTORNEY-GENERAL'S DEPARTMENT: *Australia's accession to the UN Convention on the Use of Electronic Communications in International Contracts 2005: Proposed amendments to Australia's electronic transactions laws (consultation paper),* noviembre 2008.
Disponible en:
http://www.ag.gov.au/Consultations/Documents/AustralianecommercereviewUNConventiononElectronicCommunications/UN%20Convention%20on%20ecommerce.pdf (última visita: 6/6/2014).

[431] CNUDMI/UNCITRAL: *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, 1999, párr.141 y ss.

porque sólo las firmas digitales son lo suficientemente seguras y, por tanto, pueden proporcionar el mismo nivel de seguridad que las firmas manuscritas. Así, defienden su seguridad, a la vez que las consideran como el medio más utilizado y aceptado, universalmente, para la autenticación segura de documentos electrónicos.

4.3.2.2.1. Cámara de Comercio Internacional (CCI)

La Cámara de Comercio Internacional, en un esfuerzo por facilitar y promover sistemas mundiales de comercio electrónico y firma electrónica, ha realizado varios estudios de importancia. El primero, fue GUIDEC cuya primera versión[432] se publicó en noviembre de 1997, bajo los auspicios del Proyecto de Comercio Electrónico de la CPI, con el título de *General Usage for International Digitally Ensured Commerce*.

El objetivo principal de la GUIDEC era establecer un marco general, para la autenticación de mensajes digitales, basado en la Ley y la práctica existente en los distintos sistemas jurídicos. De este modo, se trataba de proporcionar una explicación detallada de los principios, particularmente, en lo relativo a las cuestiones de seguridad de la información de sistemas, técnicas criptográficas de clave pública y emergentes capacidades biométricas. También, proporciona prácticas, estándares o recomendaciones relativas a asegurar la autenticación y procesamiento de la información digital.

La GUIDEC, a fin de profundizar en las firmas electrónicas y en la actuación de los prestadores de servicios de certificación, se centró en la firma digital; pues, en su criterio, era la que mayor valor probatorio y mayor seguridad proporciona[433]. De esta forma, define la firma digital como "una transformación de un mensaje, usando un criptosistema asimétrico tal que, teniendo una persona el mensaje *ensured* y la clave pública *ensurer* pueda determinar correctamente: 1) si la transformación fue creada usando la clave privada, que corresponde con la clave pública del firmante, y 2) si el mensaje firmado ha sido alterado desde que fue realizada la transformación".

[432] Disponible en: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/ (Última visita: 24/4/2014).
[433] FOX, W. F.: "The international Chamber of Commerce´s GUIDEC principles: private sector rules for digital signatures", *The International Lawer*, Vol. 35 – 1, 2001, págs. 71 – 78.

La GUIDEC fue actualizada en 2001, por la GUIDEC II[434], con el objetivo de establecer un marco general para la autenticación de mensajes digitales, basándose en las leyes y prácticas vigentes en los diferentes sistemas jurídicos. Al hacerlo, trató de proporcionar una explicación detallada de los principios, en particular, en lo que se refiere al sistema de información cuestiones de seguridad, técnicas criptográficas de clave públicas y emergentes capacidades biométricas; a la vez que, proporciona prácticas o recomendaciones relativas a asegurar la autenticación y el procesamiento de la tecnología digital de la información.

Por consiguiente, pasó a definir la firma digital como "una transformación de un mensaje utilizando un criptosistema asimétrico, de tal manera que, una persona que tenga el mensaje autenticado y la clave pública del firmante puede determinar con precisión: 1) si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y, 2) si el mensaje firmado ha sido alterado desde que se hizo la transformación". A su vez, define el término *authenticate* como el acto de identificarse con un mensaje; o sea, "hacer constar o adoptar un sello digital o un símbolo asociado con un mensaje con la intención de identificarse a sí mismo en relación al mensaje".

Esta definición pronostica una diferencia, que, posiblemente, se presenta irreconciliable, si bien esta definición es conforme al derecho anglosajón; pues, conforme a los foros romanistas se tiende a asociar identificación con la propia verificación de la firma[435]. De esta forma, el acto de autenticación, para la GUIDEC II, se basa en las intenciones de otros, además de la identificación mínima del firmante con el mensaje. Así, se indica que el firmante aprueba la intención de estar legalmente obligado por el mensaje, lo que queda probado a través de la autenticación y el uso de la ley, que da al mensaje un cierto efecto, que viene a ser como el acto de reconocimiento formal del firmante. La autenticación de un mensaje proporciona pruebas de que: a) el

[434] Disponible en: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC-General-Usage-for-International-Digitally-Ensured-Commerce-(Version-II)-01/10/2001/ (Última visita: 24/4/2014).
[435] CRUZ RIVERO, D.: "Análisis del concepto de firma electrónica como equivalente de la firma manuscrita", *Revista de la Contratación Electrónica*, núm. 60, mayo, 2005, pág. 3 – 122

firmante tuvo contacto con el mensaje, y b) el mensaje se ha conservado intacto desde que fue autenticado.

En 2004, la Comisión sobre Derecho y Prácticas Comerciales y la Comisión para el Comercio Electrónico, la Tecnología de la Información y las Telecomunicaciones, de la Cámara de Comercio Internacional, aprobaron un modelo de cláusulas contractuales, para permitir las comunicaciones electrónicas entre las partes y una Guía para la Contratación Electrónica[436] (e-Terms 2004): cláusulas que se proponen a las ulteriores partes contratantes, con el fin de permitir convencionalmente la utilización de las redes de ordenadores en futuras comunicaciones, en el marco del concreto acuerdo que las incluye o también para futuros contratos. Estas cláusulas están pensadas para aquellos casos, en los que las partes quieren prever en el contrato, cualquiera que sea éste su objetivo, la posibilidad de comunicarse por medios electrónicos[437].

Asimismo, la CCI pretende suministrar un instrumento para el comercio empresarial que, al dejar constancia de la voluntad de las partes, evite conflictos acerca de la existencia y validez de una comunicación, por el sólo hecho de que se hayan utilizado medios electrónicos para su remisión. Por ello, estas cláusulas sólo tienen sentido en aquellos casos en los que, el ordenamiento aplicable, no ha reconocido aún el principio de equivalencia funcional; si bien, por otra parte, solo tiene sentido cuando el ordenamiento permita la configuración convencional de esta forma jurídica[438].

En la primera clausula se viene a decir que, si bien, puede haber algunos casos en normas jurídicas obligatorias, dentro de una jurisdicción, crean barreras para la contratación por vía electrónica. En la mayoría de casos, una clara expresión de la intención de las partes contratantes, que tengan la intención de obligarse mediante un intercambio de mensajes electrónicos, indicará a los árbitros o jueces, que deciden la controversia, que voluntariamente quieren solucionar el conflicto a través de ese medio.

---

[436] Disponible en: http://www.iccwbo.org/advocacy-codes-and-rules/document-centre/ (Última visita: 24/4/2014).

[437] CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.113 - Aspectos jurídicos del comercio electrónico. Cláusulas contractuales 2004 de la CCI para el comercio electrónico (ICC e-Term 2004): Guía para la contratación electrónica*, Viena 11 a 22 de junio de 2004, págs.4 y ss.

[438] CRUZ RIVERO, D.: "Análisis del concepto de firma electrónica como equivalente de la firma manuscrita", *Revista de la Contratación Electrónica*, núm. 60, mayo, 2005, pág. 3 – 122.

Por ello, no hay ninguna razón por la que la Ley aplicable debería dejar de lado un contrato, simplemente, porque se formalizó electrónicamente.

Las e-Terms 2004 comienzan a partir de la proposición de que las partes, que coinciden en que el uso de mensajes electrónicos, dan validez y fuerza probatoria a los mismos, comprometiéndose a no impugnar la validez del contrato, por el sólo hecho de estar utilizando medios electrónicos.

Mediante la segunda cláusula se viene a establecer cuando un mensaje se considera: a) enviado, cuando entra en un sistema de información fuera del control del emisor; y, b) recibido, en el momento en que entra en un sistema de información designado por el destinatario. Cuando un mensaje electrónico es enviado a un sistema de información distinto al designado por el destinatario, el mensaje electrónico se considerará que se ha recibido, en el momento, en que el destinatario tenga conocimiento del mensaje (Cláusula 2ª, 2.2). A los efectos de este contrato, un mensaje electrónico se tendrá por expedido o enviado en el lugar donde el emisor tenga su domicilio social y se tendrá por recibido en el lugar donde el destinatario tenga su domicilio social (Cláusula 2ª, 2.3). Esta cláusula viene a repetir lo ya recogido por la LMCE en su Artículo 15, donde ya se consideraba como hecho importante, para aplicar algunas normas jurídicas; es esencial determinar el tiempo y el lugar en que se recibió la información.

Así pues, no se regula ni en qué momento o ni en qué lugar se entiende celebrado o perfeccionado el contrato, cuestión que se deja al Derecho aplicable, en cada caso en función de las circunstancias que concurran al caso concreto de que se trate[439]. Se limita a establecer unas reglas para determinar cuándo se entiende enviado o recibido un mensaje, y desde dónde se entiende enviado o recibido dicho mensaje, de tal modo que los efectos jurídicos dependerán de la naturaleza, contenido y fin del mensaje de datos. Lo que se está haciendo es facilitar la elección del tiempo y el lugar, lo caracteriza de un modo que resulte práctico y eficaz, para la aplicación de la regla nacional consagrada en

[439] MADRID PARRA, A.: "Regulación internacional del comercio electrónico: examen comparado de las leyes modelo UNCITRAL", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 2, año 2003 – 2, pág. 15 – 42.

cada caso. Incluso se hacen recomendaciones más o menos expresas, sin llegar a imponer fórmulas específicas[440].

4.3.2.2.2. American Bar Association (ABA)

La *Amercican Bar Association*[441] ha desempeñado un papel muy importante en materia de comercio electrónico y firma electrónica, hasta tal punto que sus textos han sido muy tenidos en cuenta por CNUDMI, la Cámara de Comercio Internacional e incluso ha influenciado en la regulación normativa de los Estados Unidos y la Unión Europea

Este importante papel comenzó a desarrollarse, en 1989, con la *Model Trading Partner Agreement*[442], texto concebido para el uso del soporte EDI por entidades comerciales de compraventa de bienes muebles; si bien, nada impide su utilización en actividades relacionadas con el transporte o los fletes marítimos.

Este documento trata de dejar claro para los contratantes, que suscriban un documento electrónico, que los mensajes electrónicos cumplen la misma función que los documentos en soporte papel, por tanto, serán vinculantes funcionales, de la misma manera que si el documento estuviera en soporte papel[443]. En cuanto a la firma electrónica, el documento tiene la virtud de observarla desde distintos puntos de vista: como sistema de seguridad, como sistema de autenticación para cumplimentar el requisito formal y como medio de prueba. Así, se dice que, a través de la cláusula contractual 1,5, la firma electrónica es "como una identificación electrónica, que consiste en símbolos o códigos, que han de ser adjuntos o contenidos en el Documento transmitido por cada parte, de manera que dichos símbolos o códigos sean suficientes, para identificar a la parte que originó dicho Documento[444].

---

[440] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica,* Madrid, 2009, pág. 261.
[441] Disponible en: http://www.americanbar.org/aba.html (Última visita: 26/5/2014).
[442] Disponible en: http://www.naesb.org/pdf/mtpa0397.pdf (Última visita: 24/4/2014).
[443] CRUZ RIVERO, D.: "Análisis de los antecedentes del concepto de firma electrónica como equivalente de la firma manuscrita", *Revista de la Contratación electrónica*, 2005, Núm. 60, p. 3 – 12.
[444] La Clausula 1.5 "Signature" nos dice: "Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained, where required, in the Document transmitted by such party ("Signature Code(s)"). Such Signature Code(s) shall be specified in the Appendix. In such cases where a Signature Code(s) is required for one or more Transaction Set(s), the requirement shall be specified in the Appendix applicable to such Transaction

En 1996 publicó, otro texto de importancia: *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*[445]. Se trata de un texto de carácter doctrinal, que trata de desarrollar una declaración abstracta de principios destinados a servir como base, a largo plazo, para una posible Ley de firma digital. De esta manera, define las firmas digitales, los derechos y responsabilidades de las entidades emisoras de certificados, personas a las cuales se hayan expedido certificados y partes que confían[446].

Así, define las firmas digitales como "la transformación de un mensaje usando un criptosistema asimétrico y una función hash, de modo que una persona, teniendo el mensaje inicial y la clave pública del firmante, pueda determinar certeramente: si la transformación fue creada usando la clave privada, que se corresponde con la clave del firmante; y si el mensaje inicial ha sido alterado"[447]. Por esto, la firma puede identificar al firmante cuando se concluye el acto, cuando se pueden atribuir efectos jurídicos y simplificar el documento. Se considera que la firma digital puede satisfacer todas estas funciones, incluso mejor que la firma manuscrita, en la medida que presenta una mayor capacidad para lograr: la autenticación del firmante, la autenticación del documento, la separación de los tratos preliminares de la perfección del contrato, la autenticidad del firmante y el documento con un bajo coste[448].

Como actualización de la *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, en 2003, realizó la *PKI Assessment Guidelines*[449], donde viene a desarrollar el concepto de nivel de confianza para los certificados, ante la necesidad de llevar a cabo procedimientos de autenticación,

---

Set(s). Each party agrees that the Signature Code(s) of such party affixed to or contained in any transmitted Document shall be sufficient to verify such party originated such Document(s). Neither party shall disclose to any unauthorized person the Signature Code(s) of the other party".

[445]Disponible en: http://www.signelec.com/content/download/digital_signature_guidelines.pdf (última visita: 2/10/2014).

[446] BAUM, M.: "Secure electronic commerce - II: The ABA digital signature guidelines", *Computer Law&Security Review*, Vol. 13., noviembre, 1997, p. 457 – 458.

[447] AMERCIAN BAR ASSOCIATION: *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, Chicago, 1996, pág. 9.

[448] CRUZ RIVERO, D.: "Análisis de los antecedentes del concepto de firma electrónica como equivalente de la firma manuscrita", *Revista de la Contratación electrónica*, 2005, Núm. 60, p. 3 – 122.

[449] Disponible en: http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf (Última visita: 24/4/2014).

en relación con el nivel de confianza del certificado; así, como la necesidad de que las partes que confían evalúen la idoneidad de un certificado, para un uso particular. Para los certificados de bajo nivel de confianza, es necesario llevar a cabo robustos procedimientos de autenticación, que mitiguen el riesgo de fraude.

Con este documento, la ABA trata de hacer una valoración de la infraestructura de clave pública, así como del cumplimiento de los estándares comerciales y requisitos legales. De esta manera, este estudio va dirigido a los empresarios a fin de facilitar la elección de los sistemas de seguridad, prestadores de servicios de certificación e incluso de la ley aplicable. Por ello, se pretende que sea un documento que ofrezca opiniones y observaciones sobre el proceso de evaluación de PKI, ayudando a crear un consenso en la Comunidad de Internacional para los profesionales de la empresa[450].

4.3.2.2.3. Asociación Económica de Asia y el Pacífico (APEC)

La APEC ha elaborado una serie de informes a través del *Electronic Commerce Steering Group*[451], con el fin de elaborar técnicas para la verificación de la integridad de los archivos de datos y una regulación tecnológica determinada, que pueda imponer determinados requisitos sobre las firmas electrónicas, que no existen en otros países y, por ello, limitan su uso. De esta manera, en su labor de coordinación, pide a los Estados garantizar que los usuarios tengan métodos de autenticación de una transacción, que se ajuste a sus requisitos de negocio y que estos sean aceptados de una forma uniforme por todos ellos. Para ello, propone[452]:

a) Determinar los atributos de un marco mínimo para garantizar la eficacia jurídica de los métodos de autenticación electrónica que son tecnológicamente neutrales.

[450] KIEFER, B. K.: "ABA draft PKI assessment guidelines: building consensus on PKI assessment: release of the ABA draft PKI assessment guidelines for public comment", *Computer Law&Security Review*, Vol. 17., Num. 6, 2003, p. 415 – 417.

[451] La APEC cuenta con el "Electronic Commerce Steering Group" que tiene como función promover el desarrollo y la utilización del comercio electrónico mediante la creación de marcos legales, regulatorios y de política en la región de APEC de forma transparente y coherente. De esta forma, realiza una función de coordinación en la APEC en las actividades de comercio electrónico, basándose en principios establecidos internacionalmente.

[452] Disponible en: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx (última visita: 24/4/2014).

b) Trabajar para garantizar que las leyes existentes reconozcan que la firma electrónica tiene los mismos efectos jurídicos que la firma manuscrita y sellos.

c) Dar a los usuarios a elegir el tipo de técnica de autenticación, la posibilidad de contratar con una entidad emisora de certificados de elección y el nivel de seguridad más adecuado para la operación subyacente.

d) Exhortar a las economías de la APEC a trabajar en cooperación con el sector privado, para asegurar que los enfoques regulatorios no sean demasiado específicos, de tal manera que no se impida la realización de transacciones transfronterizas.

e) Trabajar, junto a la comunidad empresarial, para identificar las estructuras del mercado a fin de incluir sistemas de autorización o acreditación de entidades de certificación.

f) Apoyar el trabajo continuo, realizado en el seno de la APEC, para desarrollar un marco legal y político uniforme de autenticación electrónica.

Sobre estas propuestas el *Electronic Commerce Steering Group*, en diciembre de 2002, desarrolla el informe[453] *Electronic authetication: iusses relating to it´s selection and use*[454]; éste se orienta hacia los Gobierno y las empresas, con el objeto de desarrollar marcos políticos, legales y económicos que permitan admitir la autenticación electrónica entre los Estados de la región.

Se define la autenticación electrónica como: el medio por el cual el beneficiario de una transacción o mensaje puede evaluar si se debe aceptar o rechazar la transacción. Se aprecia, así, dos aspectos importantes de la transacción: a) La confianza que da la

[453] Este informe se basa en una serie de documentos preparados por el *eSecurity Task Group* y su predecesor, el *Electronic Authentication Task Group*. Parte del material fue desarrollado por el Grupo de Expertos en PKI interoperabilidad, que es un subgrupo del Grupo de Trabajo de la eSecurity.

[454] GRUPO DE TRABAJO DE TELECOMUNICACIONES E INFORMACIÓN: *Electronic Authentication: Issues Relating to Its Selection and Use,* diciembre, 2002.
Disponible en: http://publications.apec.org/publication-detail.php?pub_id=486 (Última visita: 24/4/2014).

persona que envía la transacción, para demostrar que es la persona que dice ser (garantía); y, b) si la transacción tiene efecto legal en la jurisdicción del emisor o el receptor, donde, efectivamente, quiere que tenga efecto legal (efecto legal).

La confianza o la garantía, en PKI, se logra mediante la expedición de un certificado de la autoridad certificadora, que vincula una clave pública a un individuo, organización, función o atributo. La seguridad de que la unión puede establecerse, a través de un individuo, hace necesario examinar la política y las prácticas de la autoridad certificadora, lo que se evidencia a través de documentos, tales como la política de certificación, la declaración de prácticas de certificación, la declaración de la autoridad certificadora u otra documentación proporcionada por la entidad emisora. Como alternativa, un individuo puede confiar en los resultados de un tercero, la evaluación de la documentación y las prácticas de la autoridad y la determinación del nivel de seguridad. El tercero podría ser la persona, un esquema de evaluación independiente o una licencia del gobierno o sistema de acreditación, mostrando similitudes con el Artículo 7 de la Directiva 1999/93/CE.

Por otro lado, el efecto legal puede establecerse a través de escritos o acuerdos contractuales, entre las partes vinculadas en la transacción, o a través de lo establecido en la propia legislación estatal. De esta forma, se dará garantías a las partes para poder establecer sus propios estándares de seguridad y su propio efecto jurídico. Si el efecto legal se estableciera solo en la legislación, los requisitos, para establecer el efecto legal, variarán según la legislación en que se enmarque la transacción.

Como hemos dicho, en este documento se trata de establecer, como principal objetivo, la interoperabilidad a nivel jurídico y político en toda la región de Asia y el Pacífico y poder asegurar que cualquier usuario tenga acceso a un certificado electrónico y éste pueda ser utilizado con carácter transfronterizo. De esta manera, se trata de otorgar al certificado un reconocimiento recíproco como arreglo de la interoperabilidad[455], en virtud del cual la parte, que confía y que se encuentre en la zona abarcada por una infraestructura de clave pública, puede utilizar la información autorizada correspondiente a la zona de cobertura de otra infraestructura de clave

[455] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.165.

pública, para autenticar datos en la zona abarcada por la primera infraestructura de clave pública.

Por consiguiente, se hace hincapié en el marco legal establecido: la administración pública y las diferencias culturales de las economías de la APEC han dado lugar a diferentes enfoques de PKI, que actualmente impiden su aplicación. Algunas de estas diferencias son fundamentales y es improbable que se resuelvan en un futuro próximo.

Como complemento al anterior informe, en 2004, se elaboró, por el *Electronic Commerce Steering Group* de la APEC, un documento denominado: *Guidelines for Schemes to Iusse Certificates Capables of Being Used in Cross Jurisdiction eCommerce*[456], cuya finalidad fue la de realizar un examen de la interoperabilidad de los sistemas existentes y establecer unas directrices, para facilitar el establecimiento de sistemas interoperativos[457]. Este informe efectúa un examen de la interoperabilidad en los sistemas existentes, estableciendo los tipos de certificados empleados en el comercio electrónico internacional, porque se observó que cualquier enfoque desarrollado debe ser capaz de interactuar con otras normas, en particular, con las que se utilizan en Europa; pues las diferencias entre las normas pueden provocar problemas, que impidan las transacciones electrónicas y socaven el potencial regional del comercio electrónico.

Asimismo, al igual que la CNUDMI o la UE, la APEC reconoce que la tecnología PKI ha sido desarrollada en distintos países, para fomentar el comercio electrónico. Sin embargo, las diferencias entre los regímenes, que han surgido, pueden impedir el reconocimiento cruzado de los certificados en las transacciones. Por ello, tratan de aportar unos principios orientativos, mediante los cuales se anima a los Estados a facilitar la aceptación de prestadores de servicios extranjeros y promover el desarrollo de acuerdos de reconocimiento entre jurisdicciones[458].

---

[456] Disponible en: Disponible en: http://www.steptoe.com/assets/attachments/2228.pdf (Última visita: 24/4/2014).

[457] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005, pág. 7.

[458] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005, pág. 2.

Los requisitos exigidos, a proveedores de servicios de certificación extranjeros, no generan confianza para el reconocimiento transfronterizo de los certificados expedidos, ante los de sistemas de evaluación existentes; pues, no compiten en igualdad de condiciones, ya que en el mercado se encuentran entidades públicas, que utilizan estándares difícilmente reconocibles y prácticas para garantizar la interoperabilidad técnica entre los participantes, lo que suponen un sobrecoste que entorpece aún más el reconocimiento transfronterizo de los certificados.

En 2007, se elaboró el documento *Information Security Certifications Assessment Guide*[459], como complemento al elaborado en 2004, por el *Electronic Commerce Steering Group* con el apoyo del *Australian Department of Communications, Information Technology and the Arts*, que viene a ser una guía de seguridad de la información de los certificados públicos y privados, válidos en la región de Asia y el Pacífico. De esta manera, se pretende ayudar a todas las personas, físicas o jurídicas, que quieran participar en una transacción electrónica, con el fin de permitirle elegir el proveedor de servicios de certificación, que mejor le venga en el Estado en el que quieran comunicarse. Con esta ayuda se da un punto de referencia, para poder comparar y contrastar los esquemas de certificación de confianza disponibles, aumentando la seguridad entre consumidores y empresarios.

Esta guía se ha desarrollado y desplegado como un portal de Internet[460]. Este portal se utiliza como un medio de difusión de la información, ofreciendo un amplio acceso a la mayor audiencia posible[461]. No obstante, hemos de tener en cuenta que la información contenida en la web es una orientación para los usuarios. A través de este sitio web, la APEC presta un servicio a todos en la región, para hacer de este recurso una posición útil, segura y relevante del uso de las tecnologías.

El portal de Internet, del que hablamos, ha sido desarrollado por SIFT, una empresa australiana, fundada en el año 2000, líder en consultoría en el ámbito de seguridad de la información. La información utilizada en este recurso, se supone obtenida de fuentes consideradas fiables, por ello se supone correcta en el momento de

[459] APEC: *Guide to information security skill certification booklet*, mayo, 2007, núm. 207-TC-03, pág. 3.
[460] Disponible en: www.siftsecurity.net (última visita: 27/4/2014).
[461] APEC: *TEL 1/2007: Information Security certification Assessement Guide*, mayo de 2007, núm. 207-TC- 01.2, págs.2 y ss.

la publicación web; sin embargo, SIFT no se hace responsable de los posibles errores, que se hayan producido en la elaboración de esta guía.

La provisión de asesoramiento, en la web, está centrada en la seguridad de la información y los servicios seguros de certificación específicos de cada país; pues, como sabemos, cada país posee requisitos propios de certificación.

En la web se incluyen dos tipos de certificaciones:

a) Certificaciones independientes: proporcionados por organizaciones sin afiliación a ninguna tecnología en particular; siendo el objetivo principal de la página web, la presentación de las certificaciones independientes.

b) Certificaciones de proveedores: centrados en determinados dispositivos tecnológicos.

Al mismo tiempo, las certificaciones deben cumplir unos requisitos para ser aceptados:

a) La certificación debe estar relacionado con la seguridad informática.

b) Deberán rellenarse los formularios, además de aportar la documentación requerida.

c) Dejar claro el enlace web de la certificación del país de origen.

4.3.2.2.4. MERCOSUR

Para la utilización transfronteriza de las firmas y la autenticación electrónica, los Estados partes de MERCOSUR[462], han asumido, con la UE[463], una serie de

[462] Estados parte: Argentina, Brasil, Paraguay y Uruguay.

compromisos destinados a la implementación de una infraestructura técnica, de intercambio de conocimientos y de capacitación sobre tecnologías de la información.

Estos compromisos se encuadran en el denominado Proyecto MERCOSUR DIGITAL, tendente a la unificación legislativa del comercio electrónico[464]. Se trata de una iniciativa de cooperación a nivel internacional[465], entre la Comisión Europea y MERCOSUR, encuadrado dentro de un documento de estrategia regional para el periodo de 2007 – 2013. Esta iniciativa cubre los ámbitos del comercio, la economía y la cooperación y, principalmente, tienden a promover políticas y estrategias comunes, para los países del bloque en el área de la sociedad de la información.

El proyecto se estructura en dos vertientes: por un lado, se basa en la implantación de una escuela virtual para la sociedad de la información, que consiste en la implantación de una red de capacitación virtual, interconectando los países parte de MERCOSUR, para la capacitación en temas de economía digital. Por otro, se trabaja en un marco regulatorio común, para ello, se pretende realizar las siguientes infraestructuras: la creación de una autoridad certificadora de raíz en Paraguay, la creación de una autoridad certificadora de primer nivel para Uruguay, la infraestructura complementaria para una clave pública en Argentina y la infraestructura de Time Stamping para Argentina y Uruguay.

En definitiva, el objetivo es establecer directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas, así como el reconocimiento de la eficacia jurídica del documento electrónico, firma electrónica y firma electrónica avanzada en el ámbito MERCOSUR. De esta forma, se trabaja con el fin de integrar el modelo tecnológico de la infraestructura de clave pública y en un modelo tecnológico y jurídico de integración y reconocimiento mutuo de las firmas digitales.

---

[463] Decisión del Consejo de 22 de marzo de 1999, relativa a la conclusión, en nombre de la Comunidad Europea del Acuerdo marco interregional de cooperación entre la Comunidad Europea y sus Estados miembros, de una parte, y el Mercado Común del Sur y sus Estados parte, por otra.

[464] PEÑA, M.: "Proyecto MERCOSUR Digital. Apoyando a la sociedad de la información del MERCOSUR", *en II Encuentro Regional Latino Americano y del Caribe sobre Ventanillas Únicas de Comercio Exterior: avances y retos, Chile*, diciembre de 2010, pág. 1.
Disponible en: http://www.iadb.org/intal/intalcdi/PE/2011/07334a09.pdf (última visita: 30/9/2014).

[465] COMISIÓN EUROPEA – MERCOSUR. Documento estratégico regional 2007 – 2013. (2/8/2007 – E/2007/1640). Disponible en: http://eeas.europa.eu/mercosur/rsp/07_13_es.pdf (última visita: 30/9/2014).

Actualmente, no todo los Estados miembros cuentan con legislaciones, de fuente interna ni convencional, en materia de contratación y comercio electrónico, habiendo sancionado algunas Leyes, que abordan aspectos parciales de la cuestión y de forma no coincidente en muchos casos[466]. Por ello, se encuentran en plena realización de sus marcos regulatorios, así como las especificaciones necesarias, para el establecimiento de una infraestructura de clave pública y sus requisitos (autoridades de certificación, etc.)[467].

A efectos de este proyecto, hay que destacar dos resoluciones aprobadas en 2006[468]: una, las Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito MERCOSUR[469]; y otra, sobre reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito MERCOSUR[470].

---

[466] FELDESTEIN DE CARDENAS, S. L. Y BEATRIZ SCOTTI, L.: "La Convención sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales: un avance hacia la armonización legislativa en materia de contratación electrónica" en *Contratación electrónica internacional: una mirada desde el Derecho Internacional Privado* (Dir. Feldestein de Cardenas, S. L.; Coords. Andrea Medina, F.; Sofia Rodríguez, M.; y, Beatriz Scotti, L.), Buenos Aires, 2008, pág 358 y ss.

[467] Por ejemplo, por un lado, Paraguay: 5 de diciembre 2012 a cuenta con la infraestructura de la Autoridad Certificadora (AC) Raíz de firma digital, responsable por la emisión, distribución, renovación, suspensión y revocación de certificados digitales usados en la firma electrónica. El avance fue posible gracias al proyecto Mercosur Digital, que tiene como objetivo fomentar el desarrollo del Comercio Electrónico transfronterizo, por medio de la armonización de las reglamentaciones, de la infraestructura tecnológica y el intercambio de conocimientos; además, con fecha de 1 de junio de 2012 promulgo su ley de firmas electrónica y digital (http://www.mercosurdigital.org/noticias/paraguay-ya-cuenta-con-la-infraestructura-de-la-ac-raiz-de-firma-digital-promovida-por-el-proyecto-mercosur-digital/); Por otro lado, Uruguay: 5 de diciembre 2012: Uruguay cuenta con nuevas infraestructuras para el desarrollo de Comercio Electrónico en el país. Ya fue instalada, en el Ministerio del Interior, la Autoridad Certificadora (AC) de Primer Nivel, responsable por la emisión, distribución, renovación, suspensión y revocación de certificados digitales. También se ha instalado, en el data center de ANTEL, la Autoridad de Sellado de Tiempo (Timestamping) Disponible en: http://www.mercosurdigital.org/noticias/mercosur-digital-implementa-en-uruguay-la-infraestructura-para-la-emision-de-documentos-y-facturas-electronicos/ (última visita: 30/9/2014).

[468] Adoptadas por el Subgrupo de Trabajo Nº 13 "Comercio electrónico" del MERCOSUR, que ha trabajado sobre la necesidad de llevar adelante negociaciones tendentes a lograr mecanismos que posibiliten el reconocimiento de certificados digitales entre los Estados partes.

[469] MERCOSUR/GMC EXT. /RES. Nº 34/06.
Disponible:
http://gd.mercosur.int/SAM/GestDoc/PubWeb.nsf/Normativa?ReadForm&lang=ESP&id=92D972061C77BFAB032575BE0068B5E6 (última visita: 5/5/2014).

[470] MERCOSUR/GMC EXT. /RES. Nº 37/06.
Disponible:
http://gd.mercosur.int/SAM/GestDoc/PubWeb.nsf/Normativa?ReadForm&lang=ESP&id=C329A141756D589F0325760200466BCA# (última visita: 5/5/2014).

Estas resoluciones fueron adoptadas considerando que la seguridad es esencial en la generación de confianza, para el desarrollo del comercio electrónico y para la firma electrónica digital, como elemento necesario para garantizar esa seguridad.

Ambas resoluciones tienen un denominador común: la Directiva 1999/93/CE sobre firma electrónica. De esta forma, la Resolución sobre las Directrices para el reconocimiento mutuo de firmas electrónicas avanzadas, se detiene:

a) En los estándares de interoperabilidad, iguales a los establecidos por la Unión Europea, y que se sitúan en el marco de la tecnología PKI.

b) Recoge con detalle la figura del prestador de servicios de certificación, basándose en los mismos criterios fijados en la Directiva.

La Resolución sobre reconocimiento de la eficacia jurídica del documento electrónico, firma electrónica y firma electrónica avanzada, se detiene, especialmente, en la seguridad y confianza en los documentos electrónicos que requieran de la existencia de firmas electrónicas seguras; al igual que la Directiva 1999/93/CE, recoge tres tipos de firma; y al igual que el Artículo 5,1 de la Directiva, recoge una firma electrónica avanzada, basada en un certificado electrónico reconocido, que permite una mayor seguridad, denominada como firma digital.

De esta manera, se recoge el reconocimiento mutuo de las firmas electrónicas y, en principio, la libre competencia de los prestadores de servicios de certificación. Además, como el Artículo 6 de la Directiva, aseguran, como mínimo, que el prestador de servicios de certificación sea responsable por los daños y perjuicios causados.

Sin embargo, se pueden hacer varias diferenciaciones claves:

- Se atribuye a las personas jurídicas la condición de firmante.

- No se reconoce la equivalencia funcional de ninguna de las firmas electrónicas con la firma manuscrita, sino que se establece que "los documentos electrónicos satisfacen los requerimientos de la escritura".

- Están sujetos a libre competencia de los prestadores de certificación, pero se aprecia el añadido de un adjetivo: "acreditado". Ello es debido, a que se establece un sistema de control y supervisión por cualquier Estado parte de forma autónoma, en lo referente a la emisión de firmas electrónicas avanzadas, pero no en referencia a la firma digital.

Ninguna de estas Resoluciones tiene efecto práctico, por cuanto a la primera, la resolución referente a las Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas, si bien no requiere la incorporación al derecho interno, no establece un acuerdo de reconocimiento en sí mismo, sino que fija pautas a tal fin. La segunda, la Resolución relativa al reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada, requiere su incorporación al derecho interno para tener eficacia jurídica, con lo cual, representa solamente una declaración general sin efectos jurídicos, pues ningún Estado parte la ha incorporado aún[471].

Por consiguiente, queda claro que el logro de resultados en la implementación de proyectos tecnológicos, en la gestión pública, requiere una planificación adecuada y un monitoreo y una evaluación que acompañe su desarrollo; pues, el desafío al que estos países se enfrentan a la hora de implementar proyectos tecnológicos en el sector público, que permitan desarrollar el Gobierno electrónico, no se relaciona tanto con la escasez de recursos, ni con una infraestructura insuficiente, ni, tampoco, con la carencia de profesionales, sino más bien con la falta de coordinación entre las organizaciones.

Esto será suficiente para garantizar el éxito del proyecto, sobre todo en aquellos, que involucran a varios organismos; o sea, que son transversales en la administración pública. Un elemento crucial es el rol de los decisores políticos, especialmente, de aquellos que intervienen en los procesos de definición de las políticas públicas,

[471]Disponible en: http://gd.mercosur.int/SAM/GestDoc/PubWeb.nsf/Normativa?ReadForm&lang=ESP&id=C329A141756D589F0325760200466BCA# (última visita: 5/5/2014).

vinculadas al uso de las tecnologías en la administración o a la modernización del Estado[472].

4.3.2.3. Enfoque de doble nivel

El enfoque de doble nivel, también llamado enfoque híbrido, es aquel que dice ser tecnológicamente neutral, pero termina estableciendo características tecnológicas específicas, para las firmas electrónicas; es decir, la legislación establece un umbral bajo el cual exige determinados requisitos tecnológicos, para que determinados métodos de autenticación electrónica reciban una condición jurídica mínima, que les otorga un mayor efecto jurídico y, por tanto, un mayor grado de seguridad que aquellos que los cumple; un ejemplo característico de la adopción de este enfoque es la Unión Europea.

Con este enfoque se puede lograr la neutralidad tecnológica, mediante el reconocimiento mínimo de todos los tipos de firma electrónica, que se han adaptado a los nuevos desarrollos tecnológico y ofrecen un nivel de seguridad jurídica, dando un trato de favor, según el país, a determinadas tecnologías de autenticación, contribuyéndose a crear y mantener la confianza necesaria en el comercio electrónico.

En este enfoque podemos diferenciar dos grupos de países: por un lado, los que no proporcionan la suficiente flexibilidad, para la evolución natural del mercado, favoreciendo a una determinada tecnología (la firma digital), sin regular otro tipo de tecnologías alternativas; y, por otro, aquellas legislaciones que recogen disposiciones sobre la firma electrónica neutral y disposiciones relativas a características tecnológicas específicas, dando misma validez legal a ambos tipos de firma electrónica.

4.3.2.3.1. Enfoques de doble nivel con referencia a toda clase de firma electrónica

[472] CONFERENCIA IBEROAMERICANA DE MINISTROS/-AS DE ADMINISTRACIONES PÚBLICAS Y REFORMAS DEL ESTADOS: *Marco para la identificación electrónica social iberoamericana*, Asunción, Paraguay, 2011.

4.3.2.3.1.1. Singapur

Singapur, en 1998, con la promulgación de la *Electronic Transactions Act* (ETA), se convierte en el primer país en el mundo en aplicar la Ley Modelo de la CNUDMI sobre Comercio Electrónico. La ETA fue modificada, en 2010, con el fin de adaptar su ordenamiento jurídico a la Convención de Naciones Unidas sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005, que fue ratificada por Singapur el 7 de julio de 2010. Con ello, se puede afirmar que Singapur "mantiene al ritmo" de los acontecimientos que surgen a nivel internacional, al seguir la línea marcada en este contexto.

Esta Ley distingue entre firma electrónica simple (Artículo 8) y firma electrónica segura (Artículo 17). Sin embargo, lo hace de forma diferente a los demás; pues, esta Ley va más allá de la tecnología PKI y ofrece soluciones prácticas para las cuestiones, que se plantean en la utilización de medios electrónicos de comunicaciones para su celebración. Esto es apreciable, en la medida, en que la Ley, en el Artículo 8, nos dice que[473]: "cuando la ley requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica: a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; b) Si el método empleado: i) O bien es tan fiable como sea apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o ii) Se ha demostrado en la práctica que, por sí solo, o con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas".

Se trata de superar cualquier obstáculo que se oponga a la utilización de las firmas electrónicas, pero sin influir en los demás requisitos, para la validez de las comunicaciones electrónicas, a los que se refieren las firmas electrónicas. Carece de importancia que las partes estén vinculadas por un acuerdo previo, en el que se fijen los procedimientos para la comunicación electrónica como los acuerdos de asociación

[473] Transcribiendo, literalmente, el Artículo 9,3 de la Convención de Naciones Unidas sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

comercial; tampoco tiene importancia que no haya entre ellas ninguna relación contractual previa sobre la utilización del comercio electrónico[474].

Por este motivo, se puede hacer una apreciación importante: todas las firmas electrónicas, con independencia de si son o no firmas digitales o seguras, son reconocidas, de igual manera, legalmente[475]. Esta afirmación es evidente cuando en el Artículo 8 de la Ley se dice que un método debe utilizarse para identificar a la persona y para indicar la intención de esa persona y, además, dicho método debe cumplir con una prueba de fiabilidad adecuada a las circunstancias de la comunicación o demostrar en la práctica, que cumple la función de identificación y muestra la intención.

Por consiguiente, se asegura que una parte, en una transacción, no pueda invalidar el contrato celebrado por la invocación de la prueba de confidencialidad, donde la autenticidad de la firma electrónica no está en cuestión[476]. Así, cuando la identidad real y la intención de esa parte pueden ser, objetivamente, comprobadas, es indiferente que el método utilizado no sea tan fiable como apropiado en las circunstancias dadas.

Como menciona el informe emitido por IDA[477] y AGC[478], la prueba de fiabilidad hace a los Tribunales tener en cuenta más factores que los puramente tecnológicos, en el establecimiento de si una firma electrónica es o no suficiente, para identificar al firmante. La formulación de la prueba, también, es lo suficientemente flexible como para atender a los diferentes niveles de tolerancia (Artículo 8, b), i): "como apropiado para el propósito que se generó el registro electrónico, a la luz de las circunstancias). Por ejemplo, el nivel de fiabilidad, aplicable a un acuerdo de "clics", para las condiciones de uso de un sitio web, puede ser diferente del nivel de fiabilidad requerido,

---

[474] CNUDMI/UNCITRAL: *Nota explicativa a de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 148 y ss.

[475] SENG, D.: "The Singapore Electronic Transactions Act and the Hong Kong Electronic Transactions Ordinance", *Digital Evidence and Electronic Signature Law Review*, núm. 5, octubre, 2008, págs. 7 – 20.

[476] Disponible en: http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=CapAct%3A88%20Type%3Auact,areved;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DCapAct%253A88%2520Type%253Auact,areved (última visita: 5/5/2014).

[477] IDA SINGAPORE; ATTORMEY GENERAL'S CHAMBERS: *Joint IDA-AGC review of electronic, transactions act proposed amendments 2009*, LRRD No.1/2009, 30 de junio de 2009.

[478] Disponible en: http://www.ida.gov.sg/ (última visita: 5/5/2014).

con respecto a un sistema criptográfico utilizado en ejecución de las operaciones en línea.

Por otro lado, la Ley define la firma electrónica segura de forma muy similar a la firma electrónica avanzada, tal y como se recoge en el Artículo 2,2 de la Directiva 1999/93/CE sobre firma electrónica[479]. De esta forma, reconoce las firmas digitales presentando una regulación extensa y detallada de las mismas en el Anexo III. Así, las firma digitales se consideran seguras si cumplen los siguientes requisitos:

A) Ha sido creada durante el período de vigencia de un certificado válido y es verificada con referencia a la clave pública mencionada en dicho certificado.

B) El certificado se considera digno de confianza, si se trata de una unión precisa, de una clave pública con la identidad de una persona, porque:

   a. El certificado fue emitido por una entidad de certificación acreditada de funcionamiento en conformidad con el reglamento adoptado en virtud del Artículo 22.

   b. El certificado fue emitido por una autoridad de certificación reconocida.

   c. El certificado fue emitido por una agencia pública aprobada por el Ministerio, para actuar como entidad de certificación en las condiciones que se le puedan imponer.

   d. Las partes hayan acordado expresamente entre sí (emisor y receptor) utilizar firmas digitales como un procedimiento de seguridad y la

[479] MASON, S.: *Electronic Signature in Law*, Cambridge, 2012, Tabla de Casos, pág. XX.

firma digital fue verificada correctamente por referencia al remitente (clave pública).

No obstante, a todo lo anterior, en virtud del principio de la autonomía de la voluntad, piedra angular tanto de las Leyes Modelo como de la Convención, las partes en una transacción, tienen derecho a excluir el uso de las comunicaciones electrónicas y la aplicación de la Ley; también, podrán imponer requisitos adicionales más allá de lo previsto legalmente (Artículo 3 de la ETA). De esta forma, se observa como las comunicaciones van más allá del contexto contractual teniendo fuerza legal y efecto independiente, de tal manera que las partes puedan decidir sobre sus derechos y sus obligaciones[480].

Además, Singapur se adopta, no solo a la Convención, sino también, a las futuras normas que pudieran salir de la propia CNUDMI; pues, como sabemos, actualmente se está trabajando en cuestiones jurídicas relacionadas con el empleo de los documentos electrónicos transferibles. Así, en el Anexo I de la Ley se procede a realizar una lista de las transacciones excluidas[481]. Por un lado, su exclusión se debe a que no existe ningún estándar reconocido para asegurar su singularidad en el entorno electrónico; por otro, aparecen en ese apartado, presumiblemente, para facilitar una modificación en el futuro.

En este sentido, hay que señalar que aunque en el Anexo I determinados documentos y transacciones están excluidos, no se imponen a las partes; pues, la jurisprudencia tal y como se ha pronunciado en los casos SM Integrated Transware Pte Ltd vs Schenker Singapore (Pte) Ltd (2005) y Joseph Mathew y Otro v Singh Chiranjeev (2009), "no significa que haya un impedimento, para que los Tribunales

[480] SENG, D.: "The Singapore Electronic Transactions Act and the Hong Kong Electronic Transactions Ordinance", *Digital Evidence and Electronic Signature Law Review*, núm. 5, octubre, 2008, págs. 7 – 20.

[481] En el momento de la ratificación de la Convención, Singapur declaró que: La Convención no será aplicable a las comunicaciones electrónicas relativas a todo contrato de venta u otro acto de enajenación de bienes inmuebles ni a cualquier derecho sobre dichos bienes. Tampoco será aplicable a: i) la creación o ejecución de un testamento, ni a ii) la creación, el cumplimiento o la ejecución de una escritura, una declaración de fideicomiso o un poder notarial, que puedan haberse estipulado en un contrato que se rija por la Convención.
Disponible en:
http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention_status.html (última visita: 28/4/2014).

reconozcan el uso electrónico de documentos, en estos asuntos bajo la base de caso por caso"[482].

4.3.2.3.1.2. Reino Unido

El 25 de mayo de 2000, es aprobada la *Electronic Communications Act*. En el Artículo 7,2 se recoge la firma electrónica como algo en forma electrónica: a) se incorpora o asocia lógicamente con cualquier comunicación electrónica o datos electrónicos; y b) pretende estar incorporada o asociada con el propósito de ser utilizada en el establecimiento de la autenticidad de la comunicación o los datos, la integridad de la comunicación o de los datos, o de ambos[483]. En el apartado tercero del mencionado Artículo, además, se requiere que ha de haber una declaración hecha por una persona (ya sea antes o después de la realización de la comunicación), que confirme que la firma, el medio de producción, comunicación o verificación de la firma o que el procedimiento que se aplica a la firma es un medio válido para establecer la autenticidad de la comunicación o de los datos, la integridad de la comunicación o de los datos, o ambos[484].

En otras palabras, la firma electrónica se define como cualquier medio de autenticación electrónica de la identidad de una persona y de la intención de esa persona para indicar la aprobación o estar asociado con un registro electrónico[485]. De esta manera, observamos como la Ley introduce una referencia adicional, con respecto a la definición de firma electrónica dada por la Directiva en referencia a la integridad. Así,

---

[482] Joseph Mathew y Otro v Singh Chiranjeev (y Otro [2009] ASGC 51, de fecha de 29 de octubre de 2009).

[483] Artículo 7, 2 nos dice: "For the purposes of this section an electronic signature is so much of anything in electronic form as: (a)is incorporated into or otherwise logically associated with any electronic communication or electronic data; and (b)purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both".
Disponible en: http://www.legislation.gov.uk/ukpga/2000/7/contents (última visita: 5/5/2014).

[484] Artículo 7,3: "For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that:
(a)the signature, (b)a means of producing, communicating or verifying the signature, or (c)a procedure applied to the signature;
is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both".
Disponible en: http://www.legislation.gov.uk/ukpga/2000/7/contents (última visita: 5/5/2014).

[485] DAVINSON, A.: *The Law of Electronic Commerce*, Cambridge, 2009, pág. 81.

la firma electrónica debe fijarse en los datos para autenticar la comunicación o para proporcionar la identidad de la comunicación[486].

En 2002 entra en vigor la *Electronic Signatures Regulations*, que viene a dar cumplimiento a las disposiciones legales recogidas en la Directiva 1999/93/CE sobre firma electrónica. En este Reglamento se recoge la firma electrónica avanzada y la firma electrónica reconocida en los mismos términos fijados en la Directiva, a la vez que transcribe sus Anexos I y II. De esta manera, como hace la Directiva, el ordenamiento jurídico inglés establece los distintos niveles de firmas electrónica, pero haciendo una regulación separada entre ellas, aunque íntimamente conectadas.

Es decir, por un lado, *Electronic Communications Act* establece un marco regulatorio tecnológicamente neutral, con una definición de firma electrónica dispar en cuanto a sus elementos y adoptando estableciendo efectos para ésta; y, por otro, *Electronic Signatures Regulations*, recoge el resto de disposiciones exigidas por la norma comunitaria.

En este marco regulatorio establecido por Reino Unido; viendo la Directiva europea, que exige para la firma electrónica reconocida una serie de requisitos, que deben ser entendido de forma imperativa por los Estados miembros, está claro que la Ley, en la medida en se ha transpuesto en Reino Unido, parece estar en incumplimiento de sus obligaciones con la UE[487]; o sea, se observa que el énfasis regulatorio, no se pone en la firma electrónica reconocida, sino que se pone en la firma electrónica simple, poniendo en riesgo el establecimiento de la homogeneidad de las firmas electrónicas entre los Estados miembros. La principal disposición de la Directiva, el Artículo 5,1 que establece "la firma electrónica avanzada basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas", poco o nada tiene, en relación con la disposición principal de la *Electronic Communications Act*, el Artículo 7,2, donde el legislador inglés recoge la definición de firma electrónica.

[486] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.85.
[487] HEDLEY, S.: *The Law of Electronic Commerce and the Internet in the UK and Irland*, Londres, 2006, pág 254.

Asimismo, la definición dada en este Artículo tiene aspectos en común con la firma electrónica simple, definida en el Artículo 2,1 de la Directiva como "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación". Ambas tienen, un trato neutral tecnológicamente hablando, pero parece evidente que la Directiva es más genérica.

De esta forma, Reino Unido establece que una firma electrónica es una prueba admisible en cuanto a la autenticidad del mensaje o su integridad. Además, corresponderá a los Tribunales decidir en cada caso particular, si una firma electrónica ha sido utilizada correctamente y qué peso se le debe dar (por ejemplo, en relación con la autenticación o la integridad de un mensaje) contra otras pruebas[488]; no obstante, esto no significa que se le niegue valor.

Esto es así debido a que, en Reino Unido, no hay requerimientos formales para las transacciones comerciales y, obviamente, si por ejemplo un contrato oral puede considerarse válidamente hecho, no hay razón para que un contrato no pueda ser concluido usando cualquier medio electrónico, teniendo, en cualquier, caso un enfoque flexible para la aceptación de las nuevas tecnologías[489].

4.3.2.3.2. Enfoque de doble nivel con referencia especial a la firma digital

4.3.2.3.2.1. Unión Europea

La regulación comunitaria se encontró con que el problema de que la firma tradicional no era exactamente lo mismo en los distintos Estados miembros, ni siempre exigida como requisito de forma en los mismos casos, ni por las mismas razones. Por ello, la Directiva 1999/93/CE, en un principio, no aspiraba a unificar en la Unión Europea las exigencias formales de los actos jurídicos, sino que sólo, junto a la

[488] DAVINSON, A.: *The Law of Electronic Commerce,* Cambridge, 2009, pág. 81
[489] FORDER, J.: "The inadequate legislative response to e-signature", *ScienceDirect Review*, vol. 26, 2010, págs. 418 – 426.

Directiva de Comercio Electrónico[490], trataba de evitar que los requisitos formales, para estos actos, impidieran la utilización de los medios electrónicos de comunicación[491].

En este contexto, la Directiva 1999/93/CE sobre firma electrónica se promulga sobre la base de un enfoque "híbrido"[492], como un acercamiento al enfoque "minimalista" y al "prescriptivo". Este enfoque da flexibilidad, logrando una cierta neutralidad tecnológica, que no total, pues, reconoce todo tipo de firmas electrónicas que se hayan adaptado a los nuevos avances[493].

Vemos como la Directiva parte de un criterio neutral, si observamos la definición establecida en el Artículo 2,1 acerca de la firma electrónica simple, pero es evidente que rompe con la neutralidad, por un motivo claro, apreciable en el Artículo 2,2 al definir la firma electrónica avanzada haciéndolo en los siguientes términos, en el apartado c) del citado Artículo: "haber sido creada utilizando medios que el firmante puede mantener bajo su control", y en el mismo Artículo 2 apartado cuatro, nos define "los datos de creación de firma: como los datos únicos, tales como códigos o claves criptográficas privadas…".

El Considerando 8 de la Directiva recoge: los avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos. Sin embargo, del articulado de la Directiva y Anexos de la misma, se tiene presente, de forma clara y relevante, la autenticación de la firma electrónica mediante el uso combinado de un par de claves, una privada y otra pública, para cifrar y descifrar los mensajes o documentos electrónicos (basada en la tecnología PKI), haciendo referencia a la firma digital.

---

[490] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de Junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular comercio electrónico en el mercado interior.

[491] CRUZ RIVERO, D.: *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006, pág. 37.

[492] MINYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *Science Direct Review*, enero, 2007, págs. 32 - 41. En este artículo el autor nos comenta la existencia de tres tipos de enfoques: minimalista (diseñado para ser completamente de neutralidad tecnológica, es decir, no da prioridad a ninguna tecnología determinada, aso de EEUU), prescriptivo (que dan preferencia a una tecnología determinada, por lo general la basada en PKI) y el enfoque de dos niveles o Hibrido (se dice que es de neutralidad tecnológica, pero se da preferencia a una determinada tecnología.

[493] Artículo 7 de la Directiva 1999/93/CE.

Esta tecnología, por su complejidad, se ha señalado como culpable de la lenta difusión de las firmas electrónicas en Europa, si bien tienen una ventaja: utilizan el concepto de un tercero de confianza, útil para autenticar la identidad de las partes, su confidencialidad y con ello la integridad de las transacciones. A través de este tipo de firmas electrónicas se identifica a los usuarios mediante el uso de certificados digitales, verificados por una autoridad de registro (entidad que puede dar fe de la identidad de la persona que recibe el certificado) y validado por un tercero de confianza (entidad emisora de certificados)[494]. Pero el gran inconveniente que tiene esta tecnología es su alto coste. A esto hay que añadir, en referencia a la Directiva, que Ésta no puede proporcionar flexibilidad suficiente; pues, favorece una tecnología determinada, por lo que puede excluir otras alternativas tecnológicas con niveles de seguridad similares, con vistas a una innovación[495].

A nivel tecnológico, hay que hacer referencia a los programas IDA: éstos tenían por objeto facilitar la interoperabilidad, entre las redes telemáticas transeuropeas de intercambio de datos, entre las administraciones de los Estados miembros y las instituciones europeas. En una segunda fase del programa IDA, IDA II, se ha reorientado el mercado y la interoperabilidad, con vistas a aumentar la eficacia de la prestación de servicios públicos en línea, a las empresas y a los ciudadanos europeos. En una tercera fase el programa IDA II, se sustituye por el IDABC en 2004, que tiene un programa de aplicación más extenso[496]. Estos programas se han desarrollado en el marco de las transacciones transfronterizas de administración electrónica, dentro de estos programas, la acción de la autoridad de certificación ha desembocado en un proyecto piloto de autoridades de certificación puente/pasarela, que ha identificado no solo problemas tecnológicos[497], sino, también, problemas de tipo jurídico y organizativo. Esto se debe a la ausencia, en la Directiva, de disposiciones relativas a criterios para los servicios de verificación de la firma electrónica, prestados por los

[494] CARAYANNIS, E. G.; TUNER, E.: "Innovation diffusion and technology acceptance: The case of PKI technology", *Review ScienceDirect: Technovation*, marzo, 2002, pág. 840 - 859.
[495] MINYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *Science Direct Review*, enero, 2007, págs. 32 – 4.
[496] PROGRAMA IDA: Decisión Nº 1719/1999/CE; PROGRAMA IDA II: Decisión Nº 2045/2002/CE; PROGRAMA IDABC: Decisión Nº 2004/387/CE.
Disponible en: http://europa.eu/legislation_summaries/information_society/l24147a_es.htm. (última visita: 28/4/2014).
[497] COMISIÓN EUROPEA: *Informe sobre la aplicación de la Directiva 1999/93/CE*, Bruselas, 2008.

prestadores de servicios de certificación al usuario final, así como de disposiciones relativas al reconocimiento mutuo entre prestadores de servicios de certificación.

Como hemos dicho, la Directiva adopta un enfoque híbrido, lo que se aprecia en las definiciones de firma electrónica que contempla en su Artículo 2:

a) La firma electrónica simple (Artículo 2,1), "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación".

b) La firma electrónica avanzada (Artículo 2,2), firma que ofrece un nivel de seguridad mayor al anterior y que cumple los requisitos que en mencionado artículo se citan: estar vinculada al firmante de manera única, debe permitir la identificación del firmante, debe haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control y debe estar vinculada a los datos a que se refiere de modo que cualquier cambio de los mismo sea detectable.

c) La firma electrónica reconocida (Artículo 5,1), que es "la firma electrónica avanzada basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas". Que ofrece el nivel de seguridad más elevado de que los datos proceden de su supuesto remitente y de que los datos transmitidos no han sido alterados. Se concede a esta firma la equivalencia formal entre documento escrito y electrónico.

Con estas firmas electrónicas se declara la autoría de un determinado documento electrónico y se permite, a terceros, tener la certidumbre de que dicho documento les llega integro e inalterado y que el medio técnico permita transmitir de forma inalterada e íntegra un documento electrónico y determinar la identidad de su autor. Ahora bien, el legislador comunitario ha optado por conferir esa presunción de que cumplen tales

funciones cuando se utiliza el método de infraestructura de clave pública, sobre la base de criptografía asimétrica[498].

Todo ello es apreciable a través del Artículo 2,4 donde se definen los "datos de creación de firma", señalando que son: "los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica", y del Artículo 2,7 donde se definen los datos de verificación de firma electrónica: "los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica". De esta forma, el proceso de autenticación de un documento electrónico se completará con un certificado, que aportará el signatario en el que un tercero de confianza hará constar la identidad del sujeto, único titular de esa firma electrónica.

Ante las definiciones dadas en la Directiva, en el Artículo 2, es apreciable que no se recoge una definición de autenticación[499]. Lo que la Directiva entiende por autenticación debe interpretarse partiendo del Artículo 2,1, considerando, a la vez, el conjunto de artículos de la misma. Esto es así porque el legislador europeo, al igual que la CNUDMI, en el desarrollo de las Leyes Modelo sobre Comercio Electrónico y sobre Firma Electrónica, es consciente del diferente significado de "autenticación" en los ordenamientos jurídicos de los Estados miembros y la posible confusión con procedimientos o requisitos de forma concretos[500].

Sin embargo, podemos decir que la Directiva parece tratar la firma electrónica, no como una mera prueba sobre la identidad del emisor del mensaje, sino como un instrumento utilizado por las partes, desde el primer momento, con el fin identificativo; pues, la propia referencia al término "firma" debe reconducir la mera "identificación" a una función amplia[501]. Al ser la firma electrónica un instrumento utilizado, conscientemente, para identificarse en relación con un documento electrónico, explica la utilización del término "autenticación" en su Artículo 2,1. De esta forma, deja claro que

[498] MADRID PARRA, A.: "Identificación en el Comercio Electrónico", *Revista Electrónica de la Contratación*, año 2001, núm. 15, págs. 3- 60.
[499] WESTIN, R.A.: *International taxation of Electronic commerce*, La Hague, 2000, págs. 537 y ss.
[500] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 19.
[501] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, pág. 25 y ss.

la firma electrónica se utiliza, no sólo para la identificación del firmante, sino también para la autenticación de datos.

La firma electrónica simple, tal y como se establece en la Directiva, parece seguir el principio de equivalencia funcional, al establecerla como es un instrumento utilizado por el firmante para autenticar un mensaje de datos. Sin embargo, se distancia de la noción de firma manuscrita para aludir a un simple instrumento probatorio, lo que se encuentra muy lejos de los efectos concedidos a la firma electrónica, que no reúna unos requisitos especiales[502]. En esta definición de firma electrónica dota de presencia jurídica al principio de neutralidad tecnológica, acercándose, con ello, a la Ley Modelo sobre Firma Electrónica. No obstante, conforme se continúa leyendo el mencionado Artículo 2, en el apartado segundo, se observa, en la definición de firma electrónica avanzada, que realmente se está pensando en las firmas digitales[503]. Pues, solo las firmas digitales garantizan el cumplimiento de los requisitos de vinculación e identificación del firmante, de vinculación del mensaje de datos y protección de la integridad del mensaje.

La Directiva recoge el principio de neutralidad tecnológica, pero da especial importancia a un tipo de firma, la firma electrónica reconocida; haciendo girar la equivalencia formal de los instrumentos en su seguridad; es decir, en su fuerza vinculante y probatoria, situando este principio en un plano superior al del principio de neutralidad tecnológica.

De esta forma, se deduce que el efecto típico de la firma electrónica avanzada no es otro que el de crear una vinculación segura entre el firmante y el mensaje de datos y la de proteger el mensaje, pero sin que, en ningún caso, pueda equipararse esta firma a una firma manuscrita. A pesar de esto, a las firmas electrónicas simples y avanzadas no se les negarán efectos, o lo que es lo mismo, deben tener efectos jurídicos según el apartado segundo del Artículo 5, pero si se podrán negar efectos si no pueden considerarse suficientemente seguras o si no permiten establecer un vínculo,

[502] LODDER, A.R.; KASPERSEN, H. W. K.: *eDirective: Guides to European Union Law on eCommerce*, La Hague, 2002, págs. 33 y ss.
[503] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica,* Madrid, 2009, págs. 121 y ss.

suficientemente, fiable entre firmante y mensaje firmado[504]. Aunque, es obvio que las causas, por las que se le pueden negar efectos a la firma electrónica avanzada, son inferiores a las casusas de la firma electrónica simple.

Al mismo tiempo, el Artículo 5,1 de la Directiva, recoge una firma electrónica especialmente fiable, la firma electrónica avanzada, basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma, que equivale a la firma manuscrita, lo que se denomina como firma reconocida.

La firma electrónica reconocida se trata de un subtipo de la firma electrónica avanzada, caracterizada por un refuerzo de los requisitos de la firma electrónica avanzada; pues, se basa en un tipo especial de certificado (el reconocido) y necesita que la firma electrónica avanzada haya sido creada empleando un dispositivo seguro de firma electrónica. Al decir un subtipo firma electrónica avanzada, lo hacemos refiriéndonos a aquella generada por una persona física, no la jurídica. Siguiendo al Prof. Madrid Parra, esto es una opción de política legislativa; pues, se sigue el modelo de la firma manuscrita. La persona jurídica actúa a través de personas físicas, pero las consecuencias jurídicas se imputan a las personas jurídicas. Así pues, a efectos fiscales sería más operativo otorgar una firma electrónica a la persona jurídica que tiene su correspondiente código de identificación fiscal. Por ello, la ley española[505], para este concreto ámbito del derecho público, el legislador contempla la posibilidad de que el firmante sea una persona jurídica[506].

La aceptación transfronteriza de la firma electrónica solo se aplica al nivel reconocido, ya que el apartado segundo del Artículo 4 de la Directiva establece la libre circulación de los productos de firma electrónica, que se ajustan a lo dispuesto en la Directiva, lo que en la práctica significa ajustarse a los requisitos establecidos en los

[504] ALAMILLO DOMINGO, I. – URIOS APARASI, X.: "Comentario crítico de la Ley 53/2003, de 19 de diciembre, de firma electrónica", *Revista de la Contratación Electrónica*, núm. 46, febrero, 2004, págs. 3 - 64.

[505] Artículo 6,2 de la Ley 59/2003, 19 de diciembre, de firma electrónica que recoge el contenido del artículo2, 3 Directiva 1999/93/CE.

[506] MADRID PARRA, A.: "Seguridad en el comercio electrónico" en *Contratación y comercio electrónico*, (Dir. Orduña Moreno, F. Campuzano Laguillo, A.B. – Coords. Plaza Penadés, J.) Valencia, 2003, pág. 137; en "La identificación en el comercio electrónico", R*evista de Contratación Electrónica*, núm. 15, Abril, 2001, págs. 27; y en "Aspectos jurídicos de la identificación en el comercio electrónico", en *Derecho del Comercio Electrónico*, 2001, pág. 205.

Anexos[507]. La firma electrónica reconocida es un mecanismo de seguridad jurídica, emplea unas tecnologías que deben ofrecer unas garantías de calidad y seguridad elevadas, que de algún modo son "reconocidas" por los Estados miembros[508].

De esta manera, aparecen en la Directiva dos visiones diferentes de lo que debe ser la firma electrónica como equivalente de la firma manuscrita; o sea, establece una distinción entre dos tipos de firmas, las reconocidas y las demás, atribuyendo a las primeras unos efectos diferenciados. Por un lado, las firmas electrónicas reconocidas parten del hecho de que cumplen la misma función autenticadora que la firma manuscrita; por otro, las firmas electrónicas no reconocidas, plantean problemas y restricciones jurídicas, técnicas y organizativas. La Directiva define la firma electrónica avanzada de forma muy genérica, por lo que los Estados han utilizado sus Leyes para atribuirles efectos diversos con distintos niveles de seguridad, además, de imponer soluciones nacionales específicas para aplicaciones concretas, creando nuevos obstáculos al uso transfronterizo de la firma electrónica.

Por consiguiente, este estatus puede llevar a los Estados miembros, que solo están obligados a no negar efectos legales a la firmas electrónica avanzada por el hecho de estar en formato electrónico, a gozar de un mayor margen de apreciación, en cuanto a la solución de firma electrónica avanzada, o simple, y a su aceptación o no. En definitiva, el reconocimiento legal de las firmas electrónicas, que no satisfacen los requisitos del Artículo 5,1 de la Directiva, dependerán de que se llegue a probar la fiabilidad y/o la seguridad del sistema de firma electrónica utilizado, mientras queda garantizado el reconocimiento de eficacia legal a la firma electrónica, que cumpla las exigencias enunciadas en el mencionado Artículo.

Las firmas electrónicas, contempladas en el Artículo 5,1, serán siempre equiparadas a las firmas manuscritas, cuyo juicio se ha realizado *ex ante* por el legislador. Por el contrario, la eficacia de las restantes firmas estarán sometidas a un

[507] COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO EUROPEO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único*, Bruselas, 28 de Noviembre de 2008 (COM (2008) 798 final), pág. 7.

[508] ALAMILLO DOGINGO, I.: "Tipología legal de la firma electrónica en la Unión Europea", *Revista de la Contratación Electrónica*, núm. 23, Enero, 2002, pág. 32.

juicio *ex post*[509], que habrán de realizar los propios Tribunal a la espera de determinar, si son suficientemente fiables atendidas las circunstancias y si garantizan la autenticidad e integridad del mensaje de datos o documento electrónico.

La Directiva ya venía asumiendo que los Estados limitarían la eficacia jurídica y formal por el hecho de no ser lo suficientemente segura. La Directiva en su Artículo 5,2 pide a los Estados que revisen sus Ordenamientos jurídicos, para que no se niegue la eficacia jurídica a la firma electrónica por el hecho de ser electrónica, porque no se base en certificado reconocido. Es este el motivo por el que no pide a los Estados que revisen su Derecho de contratos, y es que el Artículo 5 no puede entrar en cada uno de los supuestos en los que se exige la firma, supuestos que no son uniformes en las regulaciones europeas[510].

Por otro lado, la firma electrónica reconocida es el instrumento, a través del cual se intenta conseguir la homogeneidad necesaria, para la utilización de firmas electrónicas en negocios de tracto internacional; así como, la configuración de un servicio uniforme de prestación de servicios de certificación. De esta forma, se conjuga como el equivalente pleno de la firma manuscrita a nivel europeo, incluyendo exigencias capaces de asegurar las comunicaciones electrónicas. Esta firma sirve de equivalente de la firma para legislaciones más estrictas, las medidas de seguridad que implica exceden de la propia equivalencia funcional respecto de la firma tradicional, para constituirse en garante de las comunicaciones electrónicas[511].

Sin embrago, el uso de las firmas electrónicas reconocidas plantean problemas similares a los ya esbozados para las firmas no reconocidas, si bien la situación es mucho más compleja para las no reconocidas. La firma electrónica reconocida tiene un estatus jurídico dentro de la Directiva inequívoco y se espera con ella un uso transfronterizo claro, lo que se demuestra con la presunción de equivalencia con la firma manuscrita y la obligación jurídica de los Estados miembros de reconocer mutuamente los certificados reconocidos.

---

[509] DÍAZ MORENO, A.: "Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica", *Revista de la Contratación Electrónica*, núm. 2, Febrero, 2000, págs. 45 y 46.
[510] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 188.
[511] CRUZ RIVERO, D.: *Firma Electrónica Reconocida. Análisis de los requisitos del Artículo 3,3 de la Ley 53/2009, de 19 de Diciembre, de Firma Electrónica*, Madrid, 2006, pág. 37.

No obstante, para la Comisión Europea, la falta de confianza en las firmas electrónicas procedentes de otros Estados miembros y las dificultades vinculadas a su validación han sido la principal obstaculización, para el uso transfronterizo de la firma electrónica[512]. Lo que se traduce en problemas con el propio estatus de los prestadores de servicios de certificación, que expiden certificados reconocidos en otros Estados miembros y problemas entre el firmante y el tercero de confianza, a fin de que el segundo, no pueda verificar la información contenida en la firma, lo que supone verse en la necesidad de evaluar individualmente cada firma procedente de otro Estado miembro.

En este contexto nace, el Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior[513], que deroga la Directiva. El Reglamento regula tres elementos importantes: identificación electrónica, autenticación electrónica y firma electrónica. De esta forma, amplia las funciones de la firma tal y como venían recogidas en la Directiva, de tal manera que pasa de "facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico"; es decir, de regular solo la función de autenticación o autorización de la firma electrónica, a establecer las tres funciones propias de la firma electrónica:

a) Identificación, fijando las "condiciones" para reconocer los medios de identificación electrónica (Artículo 1,a y 3,1).

b) Autenticación de la identidad, al determinarla como el "proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica o del origen y la integridad de datos en formato electrónico" (Artículo 3,5);

[512] COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO EUROPEO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único*, Bruselas, 28 de Noviembre de 2008 (COM (2008) 798 final), pág.7.
[513] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final.

c) La autenticación o autorización de la transacción, a través de la definición de la firma electrónica de persona física como "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar" (Artículo 3,10); la firma electrónica avanzada como "la firma electrónica que cumple los requisitos contemplados en el Artículo 26" (Artículo 3,11) y la firma electrónica cualificada como "una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica" (Artículo 3,12).

Asimismo, aparece una nueva figura ajena a la Directiva, el "sello electrónico", definido como "los datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos" (Artículo 3,25), que puede tener distintos niveles de seguridad, al igual que la firma electrónica. Con ello, se recoge la firma electrónica de persona jurídica, algo que resultaba necesario, ante los supuestos que se presentaban en varios ordenamientos jurídicos, en los que se recogía la posibilidad de que fueran titulares de certificados (por ejemplo, en España) lo que les creaba dudas respecto a la validez del documento del electrónico, que pudiera expedir de cara a cualquier otra empresa, ciudadano o, especialmente, a una administración.

En una relación lógica, trata primero la identificación y la autenticación, en el Capítulo II que tiene como objetivo establecer condiciones, que lleven a los Estados a un reconocimiento armonizado y a la aceptación de los sistemas de identificación electrónica a través de los Estados miembros. De esta forma, el Artículo 6 determina que donde se requiere que, cuando sea necesaria una identificación electrónica, utilizando un medio de identificación electrónica y una autenticación, en virtud de la normativa o la práctica administrativa nacional, para acceder a un servicio prestado en línea, por un organismo del sector público en un Estado miembro (como por ejemplo, en el caso de las tarjetas de e-ID o contraseñas), se reconocerá en dicho Estado miembro a efectos de la autenticación transfronteriza, en dicho servicio en línea, siempre que: a) estos medios de identificación se incluyen en una lista publicada por la Comisión Europea; b) el nivel de seguridad, de este medio de identificación electrónica,

corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público, para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica, corresponda a un nivel de seguridad sustancial o alto; c) el organismo público en cuestión, que utilice un nivel de seguridad sustancial o alto, en relación con el acceso a ese servicio en línea. Haciendo una clara referencia STORK, al que hicimos referencia en el Capítulo anterior.

Tras la identificación y la autenticación, el Reglamento determina el marco jurídico de los proveedores de servicios de confianza; tras éstos, la firma electrónica. Con esta nueva regulación trata de dar lugar a un entorno regulador previsible, al efecto de unas interacciones electrónicas seguras entre las empresas, los ciudadanos y los poderes públicos, lo que aumentará la eficacia de los servicios en línea tanto del sector público como en el privado, el negocio electrónico y el comercio electrónico en la UE.

A través del Artículo 25 se amplía el contenido del Artículo 5 de la Directiva, estableciendo una obligación explicita de otorgar a las firmas electrónicas cualificadas, los mismos efectos que a las firmas manuscritas. Además, los Estados miembros deberán garantizar la aceptación transfronteriza de las firmas electrónicas cualificadas, en el contexto de la prestación de servicios y no deben introducir requisitos adicionales que puedan crear obstáculos a la utilización de tales firmas[514]. Se trata de lograr la interoperabilidad, sin requerir una infraestructura nueva de comunicación, a través de los puentes ya existentes[515].

Este empeño regulatorio exclusivo de las firmas electrónicas reconocidas, que pasan a denominarse cualificadas, a pesar de que no siempre son necesarias en la práctica, se debe, según la Comisión Europea, a que ayudan a la gestión de la interoperabilidad y evitan el riesgo que existe en las tecnologías utilizadas en el uso de las firmas electrónicas, que, además, se entiende que está estandarizada[516]. Sin embargo,

[514] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final.
[515] TAUBER, A; KUSTOR, P KARNING, B: "Cross border certified electronic mailing: A European perspective" *Computer&Law&Security Review*, Vol. 29, núm.1, febrero, 2013, págs.28 – 39.
[516] SEALED, DLA PIPER AND ACROSS COMMUNICATIONS*: Study on the standardisation aspects of eSignature*, Bruselas, 2007, pág.9.

el Considerando 50 parece empezar a dar luz a este problema, pues reconoce que los Estados miembros usan formatos de firma electrónica avanzada diferentes, para firmar electrónicamente sus documentos por lo que considera preciso velar, porque los Estados miembros puedan soportar, técnicamente, al menos, una serie de formatos de firma electrónica avanzada, cuando reciban documentos firmados electrónicamente.

Precisamente, el Artículo 27,1 nos dice que cuando se requiere una firma electrónica avanzada con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas, las firmas electrónicas avanzadas basadas en un certificado cualificado y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos por la Comisión, mediante actos de ejecución. Se trata de reconocer formatos de firma electrónica avanzada con un nivel de garantía de seguridad inferior al de la firma electrónica cualificada, en particular, cuando un Estado miembro, en relación con el acceso a un servicio en línea, utilice este formato de firma en el sector público con arreglo a su Derecho nacional, lo que debe entenderse como una cláusula de salvaguarda respecto a las firmas electrónicas avanzadas[517], pero solo respecto de servicios públicos.

Así, se promueve el uso de estándares de firma electrónica, dentro de las recomendaciones realizadas por la UE, tratando de centrarse en un área de aplicación menos compleja y, por tanto, más accesible. Estas recomendaciones son las de promover: la interoperabilidad entre Estados miembros de la UE, el reconocimiento legal de la aplicación de la firma electrónica simple de acuerdo con la Directiva y un desarrollo sencillo en cualquier contexto empresarial. Unas aplicaciones accesibles son una condición *sine qua non* para su adopción. Las aplicaciones para el uso de las firmas electrónicas deben cumplir con unos criterios de utilización estrictos, que los usuarios deberán ser capaces de usar, a través de su firma electrónica, sin complejidad.

[517] De esta forma se hace eco de cómo las Administraciones públicas, por ejemplo, en España a través de los Artículos 10 y 15 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, prevén, en la mayoría de los casos, que los ciudadanos se puedan relacionar con ella mediante sistemas de firma electrónica no reconocida, lo que se ha llevado a Comunidades Autónomas, como la Rioja a través de la Ley 3/2002, de 21 de Mayo, para el desarrollo del uso de la firma electrónica en el ámbito de las Administraciones públicas de la Comunidad Autónoma de la Rioja. (BOE 7 – 6 – 2002).

Sin embargo, lo que se está haciendo es establecer un marco regulatorio de Gobierno electrónico, dentro de la Unión Europea, encuadrándose dentro de la globalidad de las acciones alrededor de la promoción de la sociedad de la información, lo que resulta de la aplicación del TFUE, consecuencia del Tratado de Lisboa, que otorga a la Comisión Europea competencias sobre la "cooperación administrativa"; por consiguiente, se marca un alineamiento claro de las administraciones electrónicas de los Estados miembros como un canal más de provisión de servicios gubernamentales y no como un servicio más disponible en Internet.

Por esto, las empresas podrán presentar ofertas en línea para contratos públicos en línea en cualquier lugar de la UE. Podrán firmar o/y sellar sus ofertas, además de indicar su fecha y hora por vía electrónica en lugar de imprimir y enviar múltiples copias en papel de las ofertas mediante servicios de mensajería. Las administraciones podrán reducir las cargas administrativas y aumentar la eficiencia, con lo que ofrecerán un mejor servicio a sus ciudadanos y ahorrarán dinero a los contribuyentes. Las personas que deseen hacer negocios en otro país de la UE podrán crear empresas a través de Internet y presentar informes anuales en línea, con facilidad.

Esto supone un paso adelante importante, pero no suficiente, porque de nuevo el afán regulatorio se centra en una única firma electrónica: la cualificada. Olvidándose del resto, solo mencionadas en las definiciones del Artículo 3. Así, trata de empujar a proveedores de servicios, administraciones públicas, ciudadanos, etc. en la dirección que marca la tecnología del Reglamento, ya marcó la Directiva, transmitiendo el mensaje de que la seguridad está sujeta al uso de la firma electrónica; es decir, vuelve la prescripción tecnológica y el abandono del resto de firma electrónicas, a las que no dota de ningún uso concreto.

Asimismo, en nuestra opinión, vuelven a repetirse los mismos errores del pasado; pues, contiene las mismas deficiencias que la Directiva al no tener en cuenta cualquier otro servicio, que pueda estar relacionado con cualquier otra firma electrónica, que no sea la cualificada. Es más, presuponiendo que el uso de la firma electrónica cualificada ha sido sobreestimada y siendo pronto para adelantar acontecimientos, ya que nos encontramos ante una regulación incipiente que aún no ha sido transpuesta a los

ordenamientos jurídicos nacionales, se está abriendo una vía al uso, casi exclusivo, de la firma electrónica avanzada menos segura, pero también menos costosa.

El por qué es fácil de adivinar: observemos los estudios en los que se dice que la firma electrónica cualificada requiere una aplicación muy costosa; muchas organizaciones preferirán optar por un nivel más bajo de la firma, así lo reconocía el Considerando 46 de la Propuesta de Reglamento que nos decía que los Estados miembros utilizan firmas electrónicas avanzadas o menos seguras, por ser menos costosa. Por consiguiente, en el Reglamento se menciona a la firma electrónica avanzada de la misma manera que en la Directiva, mismos efectos y misma generalidad, guardando silencio, en algunos casos, sobre los efectos que debe producir, en otros, aludiendo a ellos de manera incidental, a la hora de establecer los elementos que componen la tecnología PKI.

Por otro lado, como novedad el Reglamento recoge el sello electrónico, la firma electrónica de las personas jurídicas, que es regulada en algunos Estados miembros, como un certificado que permite dotar de garantías de autenticidad e integridad a los documentos, que se aplicaran, especialmente, en el ámbito de la Administración pública[518]. Este certificado está pensado para realizar firmas electrónicas desasistidas de forma automatizada. Las claves pueden ser almacenadas en soporte software o en un dispositivo hardware criptográfico para dotarle de más seguridad y rapidez de proceso. De esta forma, la Administración Pública es quien va a autorizar al titular de este tipo de certificado, que será solicitado por una persona física autorizada, que representará a la entidad, siendo ésta la que responderá ante la Administración de la custodia del certificado.

El Reglamento regula el sello electrónico, tratando de reforzar la confianza en las transacciones electrónicas en el mercado interior, consiguiendo una interacción segura y sin fisuras entre empresas, ciudadanos y las administraciones públicas, en el intento de incrementar la eficacia de los servicios en línea de los servicios públicos y privados, los negocios electrónicos y comercio electrónico en la Unión. Los Artículos 35 y siguientes

[518] Por ejemplo, España Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en el artículo 18,1 a) define el sello electrónico como: "un certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica".

se refieren a los efectos jurídicos de los sellos electrónicos de las personas jurídicas. Se concede una presunción legal específica a los sellos electrónicos cualificados, que deberá garantizar la autenticidad e integridad de los documentos electrónicos a los que están vinculados[519].

Un sello electrónico es, en esencia, una imagen electrónica (que puede contener número de identificación fiscal y denominación de la empresa) correspondiente a los documentos privados aportados por la empresa, con la misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia, mediante el correspondiente sello electrónico. Un sello electrónico significa que una empresa puede emitir facturas auténticas conforme a los requisitos legales de la UE.

Con esto, se pretende establecer un sello electrónico estándar de calidad, para el comercio electrónico, a nivel europeo que beneficie a las personas jurídicas, dotándolas de una mayor garantía en toda Europa. Este sello está destinado a aumentar la viabilidad de las empresas en Internet.

Los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la empresa. Si tenemos en cuenta que los principales activos de las empresas serán sus aplicaciones informáticas (equipos, software, hardware y conectividad que hacen que estén a disposición de los usuarios: correo electrónico, bases de datos de clientes etc.), con el sello electrónico se trata de poner remedio a cualquier vulnerabilidad que pueda asociarse a estos activos (por ejemplo, políticas de seguridad poco claras, software poco seguro, etc.) a través de la confidencialidad, integridad, autenticidad, disponibilidad y no repudio[520].

Este instrumento, en principio, supondrá un aumento de la confianza del consumidor europeo, ya que les será más fácil identificar a los comercios avalados con

[519] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final

[520] RUBIO VÁZQUEZ, R.; RODRIGUEZ SAU, C.; MUÑOZ MUÑOZ, R.: *La firma electrónica: Aspectos Legales y Técnicos*, Barcelona, 2004, p. 179 y ss.

dicho sello y acceder a un mayor número de productos con más seguridad. Así, las empresas podrán darse a conocer a otros países a los que hasta ahora sus productos no habían podido llegar, incrementando sus garantías.

En definitiva, este sello permitiría ejercer, con total seguridad, una de las mayores ventajas del comercio electrónico: la eliminación de las fronteras para poder llegar a un gran número de clientes, incrementándose la protección del comprador**.** Además, este sello, con mismos mecanismos que la firma electrónica de persona física, permite autenticar cualquier actuación de tráfico jurídico, especialmente, las relacionadas con la Administrativa electrónica.

a) Alemania

En primer lugar, la SigG define la firma electrónica simple (*Elektroniche Signatur*)[521], como los datos en forma electrónica, que están unidos a otros datos electrónicos o lógicamente vinculados a ellos y se utiliza para la autenticación, lo que supone que podría presentarse en múltiples formas.

En segundo, define la firma electrónica avanzada (*Fortgeschrittene Elektronische Signatur*)[522], como aquellas firmas electrónicas que son: a) exclusivas del firmante; b) pueden identificar al firmante; c) se encuentran bajo control exclusivo del firmante; y d) el documento se encuentra vinculado a la firma, de tal manera que cualquier alteración del documento puede ser detectada.

Por último, define la firma electrónica cualificada (*Qualifizierte Elektroniche Signatur*)[523], como la firma electrónica avanzada, que se apoya en un certificado reconocido en vigor, en el momento de su creación y que ha sido creada con un dispositivo seguro de creación de firma. Éstas serán las únicas que se considerarán equivalentes a las firmas manuscritas. Asimismo, prevé la aplicación analógica de las normas en materia de prueba documental para documentos electrónicos; si bien,

[521] Sec 2(1) de la SigG.
[522] Sec 2 (2) de la SigG.
[523] Sec 2 (3) de la SigG.

presume que una declaración electrónica firmada con la "firma electrónica cualificada" es auténtica[524].

La definición de firma electrónica cualificada es idéntica a la firma avanzada, basada en un certificado reconocido recogida en la Directiva, lógico si tenemos en cuenta que, la Directiva es vinculante para los Estados miembros, contempla la regulación de las firmas electrónicas en general, pero las deja olvidadas, recogiendo una regulación detallada de las firmas electrónicas que proporcionen un nivel de seguridad determinado.

Sin embargo, la Ley alemana recoge un añadido: el dato de que el certificado se encuentre en vigor en el momento de creación de la firma. Esta precisión[525] denota una especial preocupación por el problema temporal de la firma electrónica, olvidado en la Directiva. En efecto, el único medio técnico para garantizar el momento en que se generó la firma electrónica, es la utilización de un sello temporal (*time stamping*). Este sello aparece en el Considerando 9 de la Directiva como un producto de firma electrónica; no obstante, no aparece recogido posteriormente en su articulado.

Como hemos dicho, la Directiva respecto de la firma electrónica simple y la firma electrónica avanzada se limita a decir sobre ellas que no se les negarán eficacia jurídica, nada más. Lo mismo hace la Ley alemana de firma electrónica, que tras la definición en los términos mencionados, recoge la equivalencia jurídica entre las firmas electrónicas y las firmas manuscritas, sin decir nada sobre sus efectos o funciones. De esta forma, debemos acudir al conjunto de su ordenamiento jurídico para ver qué efectos pueden llegar a tener[526].

Como hemos observado, las firmas electrónicas, al igual que las firmas manuscritas, son forzosamente atributos de identidad. La función y su efecto, que tratan

[524] NÖDLER, J. N.: "Legal Framework of Electronic Signatures in the European Union and Germany", *Seminar in Network Security Institute of Computer Science Georg-August-Universität Göttingen*, 20 de febrero, 2006, págs.3 y ss.
[525] CRUZ RIVERO, D.: "Firma electrónica y documento electrónico en la nueva regulación alemana: su adaptación a la normativa comunitaria", *Revista de la Contratación Electrónica*, marzo, 2002, pág- 25 – 50.
[526] KIMMEL, F. P.: "Beweiskraft der elektronischen signatur im zivilprozess in Deutschland und österreich", *Abschlussarbeit im rahmen des ergänzungsstudiengangs rechtsinformatik an der Universität Hannover*, 11 de Julio de 2003, págs. 4 y ss.

de conseguir, son la de verificar la autenticidad del documento firmado, así como la de garantizar la integridad de su contenido, dando seguridad a las transacciones electrónicas. Por ello, en la necesaria fiabilidad exigida, en las leyes alemanas, encontramos la solución[527]. Así, en 2005, es aprobada una Ley destinada a la adopción de las formalidades de derecho privado, otras disposiciones y al tráfico de los actos jurídicos modernos; introduciendo las firmas electrónicas en el ordenamiento jurídico alemán.

De esta forma, las instituciones esenciales del comercio electrónico, documento electrónico y firma electrónica, pasan a formar parte del Código Civil alemán y en la Ley procedimental, de forma que, aunque regida por el principio antiformalista, resulta, especialmente, estricta con los requisitos exigibles a la forma escrita[528]. El Artículo 126,1 vincula la forma escrita y la firma, estableciendo que, cuando se exija aquella, debe, en todo caso, constar la firma del autor del escrito en el mismo documento. A su vez, desde el punto de vista probatorio, la conjunción del documento y firma hace prueba plena acerca de la identidad de suscriptor del documento.

Este valor probatorio, no se discute respecto de las firmas electrónicas cualificadas. Se establece, en primer lugar que las firmas electrónicas, en el sentido de la SigG, que deben ser reconocidas como jurídicamente equivalentes a las firmas manuscritas (Artículo 126 BGB), y en segundo, presume que una declaración electrónica, que se ha firmado con una firma electrónica cualificada, es una declaración hecha por el titular de la firma (Artículo 292 a ZPO).

Asimismo, se aprecia falta de referencia específica a las firmas electrónicas simples y las firmas electrónicas avanzadas, de tal manera que su valor probatorio deberá regirse por las reglas generales de la prueba, para determinar el valor que tienen como tales; partiendo del principio de equivalencia y de la no discriminación por el hecho de estar en formato electrónico. Admitido que no pueden ser discriminadas, habría que determinar la capacidad que tienen para autenticar y que garantías tienen

[527] MANNO, R.: "Le firme elettroniche in Europa", en *I Contrati di Internet: Sottoscrizione del consumatore, privacy e mezzi di pagamento* (Dir. Lisi, A.), Milán, 2006, págs.137 y ss.
[528] CRUZ RIVERO, D.: "Firma electrónica y documento electrónico en la nueva regulación alemana: su adaptación a la normativa comunitaria", *Revista de la Contratación Electrónica*, marzo, 2002, pág- 25 – 50.

para asegurar la integridad de lo contenido en el documento que se firma. Ante el vacío imperante, será el Tribunal el que decida en cada caso concreto el valor que tienen.

b) Italia

El Decreto Legislativo nº 82 de 2005, con las modificaciones introducidas por el Decreto Legislativo nº 159 de 2006, menciona tres tipos de firma en su Artículo 1[529]: firma electrónica, firma reconocida y firma digital.

La firma electrónica se define (apartado q), como un conjunto de datos electrónicos, unido o conectado a través de una conexión lógica a otros datos electrónicos, que se utiliza como método de identificación informática. Anteriormente, la definición de firma electrónica se refería a la autenticación, término que se sustituyó por el de identificación, pasando a definir la autenticación en el apartado b) del Artículo 1, como una validación de todos los datos asignados en exclusivo y de manera única a una persona, que distinguen a los sistemas de información de identidad, llevado a cabo a través de tecnologías apropiadas para garantizar la seguridad.

Por otro lado, la firma electrónica reconocida (apartado r) es la firma electrónica obtenida a través de un procedimiento, que garantice una conexión inequívoca con la persona firmante y la información de autenticación, sin ambigüedades; creada utilizando medios, que el firmante puede mantener bajo su control exclusivo y vinculada a datos, que permiten detectar si los datos han sido modificados posteriormente; basada en un certificado reconocido, creado por un dispositivo seguro de creación de firma. Esta definición es equivalente a la firma electrónica avanzada.

Finalmente, la firma digital (apartado s) se define como un tipo particular de firma electrónica basada en un sistema de claves criptográficas, una pública y otra privada, relacionadas entre sí y certificadas por un prestador de servicios de certificación y generadas utilizando un dispositivo seguro.

---

[529] MANNO, R.: "Le firme elettroniche in Europa", en *I Contrati di Internet:Sottoscrizione del consumatore, privacy e mezzi di pagamento* (Dir. Lisi, A.), Milán, 2006, págs.137 y ss.

El Artículo 21,1, del Decreto Legislativo, establece el valor probatorio de los documentos electrónicos firmados. De esta manera, establece que el documento electrónico debidamente firmado, con una firma electrónica, puede ser admitido como prueba, siendo los Tribunales quienes decidirán, caso por caso, si se admiten como prueba, lo que dependerá, entre otras circunstancias específicas posibles, de sus características objetivas de calidad y seguridad. Por otro lado, el documento electrónico, firmado con una firma digital o con una firma electrónica reconocida, tiene los mismos efectos que un documento escrito privado, presentado como prueba en procedimientos judiciales, de acuerdo con el Artículo 2702 del Código Civil italiano, a menos que el firmante aporte pruebas de que no tiene ninguna relación, en absoluto, con el documento.

El Artículo 2702 viene a decirnos que el instrumento privado es considerado como prueba, de la procedencia de las declaraciones de quien lo ha suscrito, si la persona a la que va dirigido el documento reconoce la suscripción, o si se considera legalmente reconocido[530]. El legislador prevé cuando el documento electrónico firmado con una firma electrónica digital es debido al titular del dispositivo de la firma y, así, el propietario de ésta tiene en su poder el dispositivo de creación firma.

Con esto, parece que la legislación italiana quiere decirnos, que la información firmada puede ser negada por el suscriptor aparente, con la aportación de la prueba, de modo que él no utilizó el dispositivo de firma; o, por otro lado, en sentido contrario, que la persona que recibió la información no reconoce la suscripción de la misma. Un caso de nulidad, lo encontramos en la Sentencia del Tribunal de Cantanzaro de 30 de abril de 2012[531], por la que el Tribunal viene a establecer la nulidad de determinadas cláusulas contractuales, si el consentimiento se proporciona a través de un simple "clic"; es decir, la aprobación expresa de cláusulas contenidas en el contrato on-line requieren el uso de una determinada firma electrónica, en este caso en concreto, de la firma digital[532].

---

[530] MANNO, R.: "Le firme elettroniche in Europa", en *I Contrati di Internet:Sottoscrizione del consumatore, privacy e mezzi di pagamento* (Dir. Lisi, A.), Milán, 2006, págs.137 y ss.

[531] Disponible en: http://www.ilcaso.it/giurisprudenza/archivio/7378.pdf (última visita: 1/5/2014).

[532] ITALIA: Sentencia del Tribunal de Cantanzaro, de 30 de abril de 2012, dice textualmente: "Sul quinto ed ultimo punto conviene brevemente fermare l'attenzione. L'impiego dell'equivoca dizione "firma digitale debole", a rifletterci, costituisce il classico lapsus linguae che rivela come l'estensore dell'ordinanza in esame non abbia impiegato l'espressione "firma digitale" in senso tecnico (ossia come peculiare tipologia di firma elettronica "forte" – ed anzi, "fortissima" – generata mediante l'uso di chiavi crittografiche asimmetriche, basata su un certificato qualificato e caratterizzata da ulteriori specifiche

El Tribunal viene a decirnos que una suscripción de un contrato, mediante una firma electrónica simple a través de Internet, concretamente, con un simple "clic", no es suficiente para superar la forma escrita requerida por la ley, a menos que se haga con una firma digital. Así, para superar el problema de la aceptación no habrá más remedio que descargar el formulario, imprimirlo, firmarlo y enviarlo por correo al vendedor, en caso de ausencia de dispositivos de firma digital. Sin embargo, el Tribunal no parece compartir la opinión de que el documento con firma digital pueda ser anulado, salvo en el caso previsto por el Artículo 21.2 º del Código; pues, el documento con firma digital tiene valor probatorio, aunque es posible que requieran actuaciones adicionales, después de que el firmante haya utilizado el dispositivo de firma. Lo que no será necesario si es reconocida por un notario o por otro funcionario público autorizado para ello, conforme al Artículo 2703 del Código civil.

c) España

La Ley de firma electrónica, a tenor de su Artículo 1, regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica no es una firma, sino un procedimiento electrónico que puede cumplir una función equivalente, y ahí acaba su similitud con la firma manuscrita. Nunca puede ser un acto personalísimo e inmediato, sino que es más bien un acto artificial y mediato que no se puede efectuar personalmente[533]. Ello implica las cautelas

---

tecniche), sibbene come sinonimo di "firma elettronica" la quale, questa sì, può essere sia "debole" sia "forte" (rectius: non avanzata, avanzata o qualificata) A tirar le somme, dunque, si dovrebbe concludere questo: il Tribunale di Catanzaro, dopo aver ribadito la necessità della specifica sottoscrizione della clausola vessatoria contenuta in un modulo on line, non ha (scientemente) preso posizione in ordine alla tipologia di firma elettronica necessaria ai fini dell'assolvimento dell'onere formale Va semmai soggiunto – a mo' di chiosa – che proprio la scarsa diffusione dei mezzi necessari per la generazione delle firme elettroniche (soprattutto di quelle avanzate e qualificate), ha finito per rivitalizzare l'asfittico meccanismo di tutela disegnato dall'art. 1341, comma 2, cod. civ.: vale a dire, la difficoltà tecnica di soddisfare il requisito di forma in parola è oggi di tale ostacolo alla negoziazione on line da indurre, in concreto, il predisponente a rinunciare d'imporlo all'aderente. Circostanza tanto più significativa per i contratti stipulati tra professionisti in un contesto di asimmetria di potere contrattuale qual era quello da cui la controversia ha tratto scaturigine – ai quali non si applica la disciplina di protezione dettata dal codice del consumo".

[533] COUTO CALVIÑO, R.: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista electrónica de la Contratación*, núm. 83, Junio, 2007, pág. 4 - 37.

impuestas, en el ámbito electrónico, garantizando parámetros de seguridad, como la autenticidad o la integridad del documento, que se adoptan como necesarios.

Precisamente, estudiando la firma electrónica, en el Artículo 3 de la Ley, se recogen tres tipos de firma. En el apartado primero se define la firma electrónica como "el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante". Se trata de una herramienta, que proporciona seguridad en las comunicaciones, mediante la identificación del firmante de la misma. La seguridad vendrá después, dada por la autoridad certificadora; o sea, siguiendo la terminología de la Ley, por el prestador de servicios de certificación, que vinculará un certificado expedido por éste, con los datos propios de la firma de cada usuario con su identidad, lo que garantizará que la identidad de quien envía la comunicación o el mensaje de datos.

La firma electrónica se identifica como el instrumento capaz de identificar al autor de un documento electrónico, por tanto, se acude a una definición netamente funcional, quedando supeditado el principio de neutralidad tecnológica al de equivalencia funcional[534]. Sin embargo, este precepto se está refiriendo con ello a las denominadas firmas digitales; es decir, a las firmas electrónica basada en una tecnología determinada, la tecnología PKI; pues del contexto de la Ley, y de la Directiva, está claro que se persigue una seguridad. Es por ello que, indirectamente, este precepto se está refiriendo a aquella transformación matemática de un documento, mediante una operación de cifrado con una clave, que posee una persona de modo seguro y que le vincula con ese documento que se quiere autenticar.

No debemos pasar por alto la tecnología en que se basa la firma electrónica, la tecnología PKI, que se basa en un cifrado de clave pública, formada por: certificados digitales[535]; una estructura jerárquica para la generación y verificado de estos certificados por las agencia de certificación y autoridades de registro, que cumplen las funciones de sucursales de las primeras, donde la agencia de certificación es una

[534] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 51
[535] Disponible en: http://www.cert.fnmt.es/index.php?cha=cit&sec=3&page=220&lang=es (última visita: 6/5/2014).

organización independiente y confiable[536]; directorios de certificados, que son el soporte software adecuado para el almacenamiento de los certificados; y, un sistema de administración de certificados, que es el programa que utiliza la agencia de certificación[537].

Mediante esta tecnología se restringe el ámbito en el que se pueden mover los prestadores de servicios de certificación y los proveedores de esta tecnología; o sea, el Estado puede decidir, como veremos más adelante, que dispositivos de certificación son más seguros y quien puede convertirse en prestador de servicios de certificación. De esta forma, a través del párrafo tercero del Artículo 5 se abre la vía para que operadores públicos de servicios de certificación accedan al mercado y compitan, con los operadores privados, bajo los principios de objetividad, transparencia y no discriminación, para facilitar el acceso a la firma electrónica a los ciudadanos[538].

En el apartado 2 del Artículo 3 se define otro tipo de firma electrónica, la denominada firma electrónica avanzada, que es la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, vinculada al firmante de manera única y a los datos a que se refiere en la comunicación y que ha sido creada por un medio que el firmante puede mantener bajo su exclusivo control.

Asimismo, la Guía del Ministerio de Justicia, sobre uso y eficacia de la firma electrónica la firma electrónica, la define como "aquel conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que asocian inequívocamente a un documento electrónico que permite identificar a su autor. Cuando la identificación es altamente fiable y permite detectar cualquier alteración del documento no autorizada merced a que los dispositivos empleados en la creación de la firma son seguros, por cumplir ciertas exigencias técnicas, y porque el prestador de servicios de certificación que ha intervenido está acreditado, entonces se habla de firma electrónica avanzada".

La Directiva recoge este tipo de firma en su Artículo 2,2, como ya comentamos, lo hace dando a los Estados margen para formalizar su situación, validez jurídica y

[536] Disponible en: https://www11.mityc.es/prestadores/busquedaPrestadores.jsp (última visita: 4/5/2014).
[537] Disponible en: http://www.cert.fnmt.es/index.php?cha=cit&sec=9&page=80&lang=es (última visita: 5/5/2014).
[538] Disponible en: http://www.cert.fnmt.es/index.php?lang=es (última visita: 5/5/2014).

efectos. La Ley española de firma electrónica, hace lo mismo, regula la firma electrónica avanzada de forma general. Por un lado, las Administraciones públicas[539] prevén, en la mayoría de los casos, que los ciudadanos se relacionen con ella mediante sistemas de firma no reconocida, lo que ha llevado a Comunidades Autónomas, como la Rioja[540], a regular este tipo de firma en el ámbito de las Administraciones públicas riojanas y en las relaciones entre estas y los ciudadanos. Por otro, es común el uso de la firma electrónica no reconocida, como por ejemplo en el ámbito financiero, donde la firma simple es la más utilizada, refiriéndonos con ello al "usuario y contraseña". Además, en la contratación, basándose en las condiciones "acordadas" por las partes (Artículo 3,10 LFE) las condiciones las va a determinar el predisponente, sin que la otra parte pueda negociar. En definitiva, la Ley de firma electrónica lo único que hace es repetir lo establecido en el Artículo 2,2 de la Directiva; es decir, mismos efectos y misma generalidad, y guarda silencio sobre los efectos que debe producir o alude a ellos de manera incidental, a la hora de establecer los elementos que componen la tecnología PKI.

Se trata, por tanto, de una firma que debe cumplir una serie de requisitos, que se consideran añaden calidad a la firma electrónica, siendo así una firma más segura; pues, con los requisitos descritos en el Artículo, lo que se pretende es garantizar la autenticación del mensaje firmado y evitar el rechazo en origen de los mensajes electrónicos, así como salvaguardar la integridad de los documentos electrónicos[541]. De esta forma, se llega a la conclusión de que la firma electrónica avanzada no es más que un elemento esencial para la firma electrónica reconocida. Tras establecer los tres tipos de firma electrónica, la Ley de firma electrónica abandona a su suerte a la firma simple y avanzada, para destinar toda su ambición regulatoria a la reconocida, a la tecnología empleada, sus efectos y, desde una perspectiva subjetiva, al prestador de servicios de certificación, actitud compartida por la Directiva[542]. La Ley se detiene en la firma reconocida, única clase de firma electrónica legalmente asimilable, en términos de equivalencia funcional, a la firma manuscrita. Todas las funciones propias de la firma

[539] Artículos 10 y 15 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
[540] Ley 3/2002, de 21 de Mayo, para el desarrollo del uso de la firma electrónica en el ámbito de las Administraciones públicas de la Comunidad Autónoma de la Rioja. BOE 7 – 6 – 2002.
[541] MARTÍNEZ NADAL, A.: "Firma electrónica, certificados y entidades de certificación. La Ley 59/2003 de firma electrónica" *Revista de la Contratación Electrónica*, núm. 47, Marzo, 2004, pág. 83.
[542] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 101.

electrónica residen en la denominada firma electrónica reconocida: identificación, atribución, privacidad, integridad y seguridad. Lo que no acontece con las firmas electrónicas simple y avanzada.

La firma electrónica reconocida se define en el Artículo 3,3 de la Ley, definición que aparece como relevante ya que el Artículo 3,4, a efectos de reconocimientos de validez y eficacia a la firma electrónica, equipara la firma electrónica reconocida a la firma manuscrita, mientras el Artículo 5 de la Directiva realiza tal equiparación respecto de la firma electrónica avanzada que cumpla determinadas exigencias. Pero, la firma electrónica reconocida, más que un nuevo concepto de firma, basado en el establecimiento de nuevas exigencias inherentes a la propia firma, es un término en el que se agregan los distintos requisitos extrínsecos a la propia firma electrónica avanzada ya existente, para que tenga plena validez y eficacia; pues, la firma electrónica reconocida no es más que una firma electrónica avanzada, basada en un certificado reconocido en un dispositivo seguro de creación de firma y estos son los requisitos para el reconocimiento de efectos que debe cumplir la firma electrónica según el artículo 3,4 de la Ley y el Artículo 5 de la Directiva[543].

Esta equiparación se encuentra limitada tanto en el ámbito privado como en el ámbito público. En el ámbito privado, la equiparación queda supeditada al juego de la autonomía de la voluntad, en la medida en que las partes pueden consentir la utilización de la firma electrónica, como mecanismo de expresión del consentimiento, tal y como puede apreciarse en el Artículo 3,10 de la Ley; y en el ámbito público, la limitación se encuentra, en cuanto que su utilización, en aquellos procedimientos en los que se autorice y respeten las condiciones adicionales que se impongan, tal y como se aprecia en el segundo párrafo del Artículo 4,1 de la Ley.

Por ello, la firma electrónica reconocida no parece tener reconocimiento real[544]; pues, de poco sirve decir que la firma electrónica reconocida equivale a la firma manuscrita, si no se prevé ninguna posibilidad real de uso de esa firma. Esto se ha de

[543] MARTÍNEZ NADAL, A.: "Firma electrónica, certificados y entidades de certificación. La Ley 59/2003 de firma electrónica", *Revista de la Contratación Electrónica*, núm. 47, Marzo, 2004, pág. 84 y ss.

[544] ALAMILLO DOMINGO, I – URIOS APARASI, X.: "Comentario crítico de la Ley 53/2003, de 19 de diciembre, de firma electrónica" *Revista Electrónica de la Contratación*, núm. 46, Febrero, 2004, pág. 35.

hacer a través de la imposición a los sujetos intervinientes, en el tráfico jurídico, de la obligatoria admisión de la firma electrónica reconocida en las operaciones en que intervienen. El marco para hacerlo sería el Código civil, tal y como ha hecho Alemania, introduciendo la firma electrónica dentro de los textos básicos de su Ordenamiento jurídico.

Teniendo como referente el BGB, junto con otras normas y lo acontecido en Alemania en referencia, por supuesto, a la firma electrónica, armonizó su Derecho con las nuevas tecnologías. El Código civil en España, es horizontal en todo el sistema, así, si se modificara el Código civil se podría garantizar la equivalencia funcional en todo el sistema.

Por otro lado, la firma electrónica, que equivale a la firma manuscrita, presenta un nivel de seguridad muy superior al de la firma manuscrita, de modo que si le añadimos su capacidad de asegurar la integridad y confidencialidad del mensaje, esta firma electrónica se encuentra con un valor añadido, como garante de la seguridad de las comunicaciones. Lo que nos lleva a pensar que su configuración, frente a la firma manuscrita, desdibuja la equivalencia funcional entre ambas instituciones, ya que si la firma electrónica es un medio de autenticar los datos, como la firma manuscrita, en algunos casos, un medio para firmar un documento, es posible que sea también algo más que la firma manuscrita; es decir, una institución ordenada a la salvaguarda de la seguridad de las relaciones a través de Internet[545].

Esta firma electrónica se apoya en la denominada tecnología PKI, gestionada por un prestador de servicios de certificación, que permite asegurar, incluso con mayores garantías que el papel y la firma autógrafa, la identificación del firmante y la atribución de los mensajes. Lo que nos lleva a afirmar, que la firma electrónica reconocida es el mero resultado de la tecnología actualmente disponible y comercializada, así: ¿qué pasaría si en el futuro nuevas tecnologías superasen o sustituyeran la tecnología PKI?; o mejor dicho: ¿tendrían cabida en nuestro ordenamiento otra tecnología más simple o sencilla, o, al contrario, otra tecnología más segura u otra más fiable?.

[545] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 127.

Si lo importante es que el instrumento sea seguro, no tendría ningún sentido privar de eficacia formal a las firmas electrónicas igualmente seguras, pero que no cumplen los requisitos del Artículo 3,3 de la Ley. De esta manera, ante este problema de neutralidad tecnológica, respecto de otro instrumento electrónico que sea igualmente seguro, puede plantearse un problema de equivalencia funcional respecto de la firma manuscrita; además, es posible que, aun no siendo tan segura como la firma electrónica reconocida, una firma electrónica sea capaz de satisfacer el requisito de seguridad, equivalente al exigido para una firma manuscrita.

Como ya dijimos, la Ley Modelo sobre Comercio Electrónico, en su Artículo 7, se basa en el reconocimiento de las funciones que cumple la firma manuscrita en el soporte papel. En conexión y complemento a este Artículo, la Ley Modelo sobre Firma Electrónica ofrece normas prácticas, para comprobar la fiabilidad técnica de las firmas electrónicas, estableciendo un vínculo entre dicha fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica. Como vimos antes, esta Ley Modelo tiene por finalidad mejorar el entendimiento de la firma electrónica y la seguridad técnica en operaciones de importancia jurídica, formulando el llamado principio de importancia relativa, consistente en que los requisitos de seguridad deberán ser proporcionales a la transcendencia de la comunicación y a la cuantía económica del negocio jurídico efectuado, de modo que el medio electrónico pueda utilizarse para negocios de pequeña entidad, que quedarían excluidos del mercado virtual por antieconómicos[546].

La Ley española de firma electrónica, al incorporar al derecho interno la Directiva europea, aprecia este principio, pero en el establecimiento de una tecnología determinada y una firma electrónica concreta, haciendo girar la equivalencia formal de la firma electrónica entorno a su seguridad; es decir, en su fuerza vinculante y probatoria, persiguiendo la seguridad de los instrumentos con el fin de dar seguridad a las transacciones. Esto es así, porque teniendo en cuenta el Artículo 3,9, que establece que no se negarán efectos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida, en relación con los datos a los que esté asociada, por el mero hecho de presentarse en forma electrónica. Siguiendo el criterio del Prof. Cruz

[546] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 131.

Rivero[547], lo que se hace es un reconocimiento a la naturaleza de la firma electrónica, guardando silencio sobre la eficacia y efectos jurídica de las firmas electrónicas, debiendo establecer caso por caso la equivalencia del resto de las firmas, no de la reconocida. Quedando en manos de los jueces el que esta situación no lleve al absoluto casuismo.

La firma electrónica basada en la tecnología PKI parece, hoy día, la única que produce un elevado grado de certeza a los efectos de atribución, identificación, privacidad, seguridad e integridad del mensaje de datos, que las prácticas y usos internacionales requieren, para la firma electrónica reconocida. Así, el legislador español opta por establecer esta tecnología, lo cual no es nuevo, ya que todo viene del obligado cumplimiento de la Directiva 1999/93/CE. Sin embargo, en 2001, se demostró que la tecnología cuántica podía romper todos los esquemas de la firma digital[548]. Si bien aún se está lejos de sustituir la tecnología PKI, las legislaciones comienzan a estar en jaque ante la posibilidad de quedar anticuadas.

4.3.2.3.2.2. China

La Ley de Firmas Electrónicas de la República Popular de China tiene como objeto estandarizar el comportamiento de la firma electrónica, su validación legal y la protección de los derechos e intereses legítimos de las partes interesadas. Para ello, se inspira, fundamentalmente, en las Leyes Modelos y, especialmente, en la Ley de Transacciones Electrónicas de 1999 de Singapur.

La firma electrónica se define en el Artículo 2 como "los datos en forma electrónica incluidos y unidos en un mensaje de datos, que pueden ser utilizados para identificar al firmante, en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos"[549].

---

[547] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 187.

[548] BUCHMAM, J: "Post-quantum signatures", *Invited talk Darmstadt University of Technology. Germany*, 30 de septiembre de 2004.
Disponible en: http://itslab.csce.kyushu-u.ac.jp/iwap04/PostQuantumSignatures.pdf (última visita: 1/5/2014).

[549] "Article 2: Electronic signatures in this law refer to data that are included or attached in electronic data for identification of the signer and for proof that the signer agrees with the included contents.

Esta definición, a simple vista, podría decirse que es similar a la recogida en la Ley Modelo sobre Firma Electrónica. No obstante, a través de la expresión "los datos incluidos y unidos" (asociados), limita la vinculación por la cual una firma electrónica puede estar unida a un mensaje de datos[550]. De esta manera, la definición puede ser interpretada de forma restrictiva, hasta el punto de poder crear confusión y provocar, que los tribunales puedan excluir aquellas firmas, que se envían de forma separada respecto del mensaje de datos, pero asociado a éste. Observemos que esta restricción es apreciable en todas las legislaciones, salvo en Singapur, que muestra el lado más natural de la transacción.

Lo que nos lleva a pensar que se limita a establecer un marco legal para el entorno electrónico, no cubriendo todos los aspectos de usos posibles de los mensajes de datos y las firmas electrónicas en el comercio electrónico. Por otro lado, la ley establece el principio de equivalencia funcional, reconociendo a la firma electrónica y los mensajes de datos la misma validez jurídica que si de firmas o contratos manuscritos se tratara, de tal manera que no se le negaran efectos jurídicos por el hecho de estar en forma electrónica (Artículo 3), siendo aplicable solo a la firma electrónica fiable (Artículo 14).

La fiabilidad de la firma electrónica "simple" se habrá de determinar caso por caso, si nos atenemos al Artículo 8 de la Ley, donde en su apartado primero, nos dice que, al valorar la fuerza probatoria, se tendrá en cuenta la fiabilidad de la forma en que se generó, almacenó y transmitió el mensaje de datos y se identificó a su iniciador. En los casos en que se requiera la prueba electrónica, el Tribunal obligará a las partes a proporcionar lo que estimen oportuno, para demostrar la autenticidad, fiabilidad y originalidad de la comunicación electrónica, de lo contrario se le podrá negar su valor[551].

A pesar de que la prueba electrónica es admitida como tal en los procedimientos judiciales, su valor probatorio no es seguro y tiene que ser respaldada por otras pruebas,

---

Electronic data in this law refer to information that is created, sent, received, or preserved via electronic, optical, or magnetic tools or similar media".

[550] WANG, M.: "Translation and introduction to the Electronic Signature Law of China", *Digital evidence and Electronic Signature Law Review*, núm. 2, octubre 2005, pág. 79 - 94.

[551] WANG, M.: "Electronic evidence in China", *Digital evidence and Electronic Signature Law Review*, núm. 2, octubre 2005, págs. 45 - 50.

generando incertidumbre. Lo que supone la generación de un marco claro de desconfianza en los medios electrónicos, que de una forma u otra contagia a los usuarios, generando desconcierto en las propias transacciones que pretenden realizar, lo que puede llevar a optar por cualquier otro medio disponible, antes que el electrónico. Por ello, ante la definición dada y con el reconocimiento del principio de equivalencia funcional, parece que se opta por un criterio neutral, tecnológicamente hablando, tal y como se recoge en las Leyes Modelos.

Sin embargo, lo cierto es que adopta un enfoque híbrido, concediendo un grado de privilegio a la firma digital, de tal manera que la Ley, en su Capítulo tercero, que en referencia a la fiabilidad de la firma electrónica, nos dice que solo lo será si cumple una serie de requisitos prescritos[552] y, así, solo de esta manera se podrá considerar la firma electrónica como tal.

Finalmente, la Ley concede a las partes autonomía para elegir la firma electrónica. No obstante, con el establecimiento de requisitos de confiabilidad, establecidos en los Artículos 13 y siguientes, que recuerdan mucho a los establecidos en la Directiva 1999/93/CE sobre firma electrónica para las firmas electrónicas avanzadas, se rompe con el principio de neutralidad tecnológica, instaurada en la definición dada inicialmente. Ante la imposibilidad de garantizar una seguridad absoluta, contra el fraude y el error en la transmisión, el legislador intenta formular unos principios que lo llevan a prescribir una tecnología determinada, la tecnología PKI o infraestructura de clave pública. Esta prescripción se puede hacer de distinta manera, según el grado de intervención estatal. En el caso de China, la intervención es total, pues fijándonos en su normativa, especialmente en el Artículo 18, todo gira en torno a una autoridad central, el Ministerio de Industria de la Información, que será quien decida si emite la licencia o no al prestador de servicios de certificación.

[552] WANG, M.: "Translation and introduction to the Electronic Signature Law of China", *Digital evidence and Electronic Signature Law Review*, núm.2, octubre 2005, pág.79-94.

4.3.2.3.2.3. Argentina

En 2001, se aprobó la Ley 25.506 sobre Documento Electrónico y Firma Digital (LFD), necesaria para validar la autenticidad y no repudio del documento electrónico.

Esta Ley, en su Artículo 1, reconoce el empleo de la firma electrónica y la firma digital, así como su eficacia jurídica en las condiciones establecidas. Ambas firmas se definen por separado: la firma digital en el Artículo 2 como "el resultado de aplicar a un documento electrónico digital, un procedimiento matemático, que requiere información de exclusivo conocimiento del firmante, encontrándose bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultánea, permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma"; y la firma electrónica en el Artículo 5 como "el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como medio de identificación, que carezcan de alguno de los requisitos legales para ser considerada firma digital".

De estas definiciones podemos deducir que la Ley está tratando ambas firmas de forma separada, estableciendo dos tipos de firma electrónica claramente diferenciadas. Por un lado, el Artículo 5 está estableciendo un concepto de firma amplio que puede abarcar toda clase de identificación, por ello será firma electrónica, aquella que no reúna los requisitos para ser considerada como firma digital; o sea, los requisitos del Artículo 2 y del Artículo 9 de la Ley. Además, el que quiera hacer valer la firma electrónica debe demostrar su validez, de no hacerlo, la firma electrónica será inválida, ya que no impera a su favor la presunción de autoría e integridad (Artículos 7 y 8, respectivamente), que se establecen para la firma digital.

Por otro lado, a la propia firma digital, se le da un concepto ajeno a la Directiva 1999/93/CE, sin perjuicio de que este tipo de firma pueda quedar reconocida como la firma electrónica avanzada[553]; pues, en el desglose del contenido, del mencionado

[553] CRUZ RIVERO, D.: "La firma electrónica", en *Derecho del comercio electrónico* (Dir. Illescas Ortiz, R.; Coord. Ramos Herranz, I.), Buenos Aires, 2010, págs. 490 y ss.

Artículo 2, podemos encontrar en gran medida los mismos requisitos que en la Directiva europea:

a) Permitir identificar al firmante y detectar cualquier alteración del documento digital.

b) Se genera mediante la aplicación al documento digital que se pretende firmar con un procedimiento matemático.

c) Se genera un procedimiento que requiere información de exclusivo convencimiento del firmante y que se encuentra bajo su control absoluto.

En cualquier caso, la firma digital sólo será válida si cumple los requisitos de validez del Artículo 2 y del Artículo 9 LFD; además, hay que adjuntar otros requisitos, en referencia a la equivalencia con la firma manuscrita (Artículo 3), presunción de autoría, a tener muy en cuenta, introduciendo el concepto de certificado digital, de donde resulta, que no hay firma digital si no hay certificado digital (Artículo 7) y presunción de integridad: "salvo prueba en contrario" el documento digital no ha sido modificado desde el momento de su firma (Artículo 8). De esta forma, vemos como la Ley argentina hace referencia, al igual que la Directiva europea, a una tecnología determinada de claves asimétricas (tecnología PKI). Sin embargo, contiene una diferencia significativa con la misma, no hace referencia a la autenticación del documento como parámetro definidor de la firma[554].

En La Ley española tampoco lo hace, pero de su contexto se puede desentrañar el significado de autenticación, si vemos con detalle el artículo 3,1 la expresión "pueden ser utilizados como medio de identificación del firmante", ampara las limitaciones de los mecanismos de autenticación[555], lo que crea inseguridad. Así, la LFD, en principio,

[554] CRUZ RIVERO, D.: *Eficacia formal y probatoria de la firma electrónica*, Madrid, 2006, pág. 32: "Cabe entender que la identificación implica la designación de una persona de forma no ambigua; mientras que la autenticación se refiere a un elemento intencional que permite a una persona dar a conocer su voluntad de aparecer ligado al acto que ella misma ha creado".

[555] ALAMILLO DOMINGO, I. – URIOS APARASI, X.: "Comentario crítico de la Ley 53/2003, de 19 de diciembre, de firma electrónica", *Revista de la Contratación Electrónica*, núm. 46, Febrero, 2004, págs. 3 - 64.

presenta el mismo problema que la española, crea mayor inseguridad a través de la presunción de su Artículo 7.

Este Artículo 7 hace fiel reflejo de la realidad con su presunción de autoría, distinguiendo en el ámbito electrónico entre las figuras que pueden confluir o no como firmante: solicitante (el que solicita un certifica de firma electrónica), suscriptor (persona que tiene derecho a usar ese certificado y aparece identificada con el mismo), y firmante (persona que efectivamente genera la firma)[556]. Pero no es realmente así, si bien, el firmante tiene la obligación estricta de ejercer el control exclusivo sobre el dispositivo de creación de firma (Artículo 25).

Como decíamos, elemento esencial de la firma digital es el certificado digital para dar efectos jurídicos; es decir, no puede haber firma digital sin certificado digital; asimismo, no habrá certificado digital si no hay un certificador licenciado, término equivalente al prestador de servicios de certificación en Europa. De esta forma, el certificado digital se concibe como un instrumento al servicio de la firma digital, para la exigencia de equivalencia con la firma manuscrita, por exigencia del Artículo 3; aunque, a diferencia que en España, no se hace se hace distinción entre certificados reconocidos o no reconocidos, debiéndose acudir al Artículo 14 para identificar la seguridad del certificado digital, que ha de contener como mínimo los siguientes requisitos:

a) Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando el período de vigencia y los datos que permitan su identificación única.

b) Ser susceptible de verificación respecto de su estado de revocación.

c) Diferenciar claramente la información verificada de la no verificada, incluidas en el certificado.

d) Contemplar la información necesaria para la verificación de la firma.

[556] COUTO CALVIÑO, R.: "Reflexiones de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista de la Contratación Electrónica*, núm. 83, Junio, 2007, págs. 4 - 37.

e) Identificar la política de certificación bajo la cual fue emitido.

Ante este contenido mínimo, y observando informe de la Comisión redactora de la Ley[557], podemos ver, de manera lógica, la posibilidad de que estemos ante certificados digitales en su forma más simple o en su forma más segura, lo que nos sitúa, en nuestra opinión, en un posible tercer tipo de firma electrónica, la firma digital válida, o ante una situación en la que se le deja, a la parte más débil, o tercero de confianza, la obligación o trabajo de verificación, en situación de clara inseguridad, aunque quede recogido que se ha diferenciar la información verificada de la no verificada por el certificador. Lo que está claro es que la identificación del titular va a ser verificada (Artículo 14, b-1 LFD), pero nada más se dice en la Ley, salvo la exclusión de la responsabilidad prevista en el Artículo 39, c) del certificador en referencia a los datos no verificados.

Esto se puede apreciar atendiendo a la lista amplia de obligaciones a cumplir el prestador de servicios de certificación; pues, pueden plantearse problemas de diferente índole, ya que la LFD no se refiere, exclusivamente, a la responsabilidad del certificador licenciado, sino que habla del "certificador", lo que hace intuir la existencia de dos tipos de sujetos responsables, el certificador licenciado y el simple certificador, a estos últimos se les aplicará haciendo extensibles estas reglas generales de responsabilidad recogidas en los Artículos 37 a 39 LFD, pero hemos de dejar claro que estos no tienen un marco regulatorio bien definido en la Ley; ya que no existe regulación alguna sobre esta materia. Es decir, no se regula al certificador que puede emitir certificados digitales con efecto de firma electrónica, utilizando tecnología de firma digital.

4.3.2.3.2.4. Chile

En Chile, el 12 de abril de 2002, se publicó la Ley Nº 19799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, que establece:

[557] LYNCH, H. M.: "El documento y la firma digital en el Derecho Argentino", *Revista Anales de Legislación Argentina*, Boletín Informativo, 2001, núm. 34, pág. 11.

a) En el Artículo 1 su ámbito de aplicación: regula los documentos electrónicos y sus efectos legales, el uso de la firma electrónica y los prestadores de servicios de certificación, así como el procedimiento de acreditación de estas entidades.

b) En el Artículo 2 y siguientes contiene un listado de definiciones de los conceptos fundamentales y regulación de sus efectos.

El Artículo 1,2 nos dice textualmente: "Las actividades reguladas por esta Ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte papel". Con ello, se hace hincapié en los principios inspiradores del comercio electrónico y en base a los cuales se elaboró la Ley Modelo sobre Comercio Electrónico: la equivalencia funcional y la neutralidad tecnológica.

La equivalencia funcional se recoge en el Artículo 3, de forma que, al igual que en la Ley española, se reconoce que los actos o contratos, otorgados o suscritos por medio de firma electrónica, serán válidos y producirán los mismos efectos que los celebrados por escrito y en formato papel. Se trata de abarcar todos los usos tradicionales de la firma manuscrita con consecuencias jurídicas, siendo la identificación del firmante y la intención de firmar, el mínimo del que se parte, a tenor de las definiciones del Artículo 2.

En cambio, la neutralidad tecnológica, sin bien se recoge en el mencionado precepto, no se respeta finalmente, pues en la distinción de firma electrónica y firma electrónica avanzada se recoge la tecnología PKI. En la definición de la firma electrónica (Artículo 2, f), satisface la función de identificación del firmante y mantiene la observancia de la neutralidad tecnológica, dejando libertad a los operadores del comercio y a todo interesado, para suscribir o no documentos con este tipo de firma.

La firma electrónica avanzada Artículo 2, g), es una firma que se asemeja en gran medida a la firma electrónica avanzada de la Ley española, y por tanto a la Directiva 1999/93/CE. Sin embargo, como dice el Prof. Sandoval López, más completa, si bien describe todas las funciones de seguridad de una firma electrónica, incluido el no

repudio[558]; aunque, en cualquier caso, de lo que no cabe duda es que ambas han recogido la tecnología PKI. Se hace necesaria la existencia de prestadores de servicios de certificación que ejecuten una labor de confianza general en todo el sistema.

Estas entidades se definen, en el Artículo 11, como las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan prestar y están sujetos a un gran número de obligaciones descritas en el Artículo 12. Así, el grado de diligencia que se le pide es muy alto, siendo un régimen en ocasiones de responsabilidad objetiva, pero aún así, el prestador de servicios de certificación puede quedar exento de responsabilidad, si demuestra que actuó con diligencia debida.

De la definición, así como del Artículo 15 sobre certificados de firma electrónica, observamos como los certificados podrán ser emitidos por entidades no establecidas en Chile y que serán equivalentes a los otorgados por prestadores de servicios del país, no obstante, se establece que habrán de ser homologados por estos bajo su responsabilidad, y para ello habrán de observarse los requisitos establecidos en la Ley y en su Reglamento, en virtud de acuerdo internacional ratificado por Chile

4.3.3. Visión de conjunto

Como puede apreciarse, existe una intensa actividad legislativa sobre la firma electrónica, destinada a la adopción de medidas, para sustituir a la firma manuscrita, considerando aquella como equivalente a ésta última. No obstante, cada Estado ha adoptado un enfoque o modelo legislativo: minimalista, prescriptivo o de doble nivel.

Los tres enfoques vistos tienen, en común, la importancia de la autenticación de la firma electrónica en la transacción, en el comercio electrónico. Se puede decir que todas son válidas, con sus ventajas y sus desventajas. No obstante, en un contexto internacional, en el que el mercado y la tecnología están en un desarrollo constante, parece más lógico el establecimiento de un marco neutral; pues, la legislación, con

[558] SANDOVAL LÓPEZ, R.: "Análisis de la Ley Nº 19.799, de Firma Electrónica de la República de Chile", *Revista de la Contratación Electrónica*, núm. 32, Noviembre, 2002, págs. 21 – 37.

orientación tecnológica, tiende a originar una mezcolanza de normas técnicas y requisitos de autorización contradictorios, que dificulta mucho la utilización transfronteriza de las firmas electrónicas, de la misma manera que los prestadores de servicios de certificación, que las autentican, están sujetos a requisitos jurídicos y técnicos contradictorios en los diferentes ordenamiento.

De esta forma, una consecuencia previsible en la legislación, que facilita una específica tecnología, es que la norma regula unos requisitos para favorecerla. Desde este punto de vista, ante lo estudiado hasta ahora, se va, en la mayoría de los países, hacia la seguridad de la información, a través de una tecnología concreta. Esto supone una solución individual, que da un respaldo particular, a través de desarrollos técnicos, con enfoques de gestión centralizada, a través de entidades públicas, en la mayoría de los casos, lo que representa, a priori, opciones de diseño, que están lejos de ser las apropiadas para la aplicación internacional de la firma electrónica.

Fijémonos por ello, en lo que se dice de la firma, por un lado, existe un consenso general de que se le debe dar validez legal a la firma electrónica; aunque todas las normas comparten el mismo objetivo: facilitar el desarrollo de las tecnologías de firma electrónica y el comercio electrónico; por otro, hay poco acuerdo sobre la manera de lograr este objetivo: en la descripción de las intención del firmante y su autonomía de la voluntad; en la identificación, que se quiere lograr, en muchos casos, con el uso de la criptografía asimétrica; en el trato de las coordenadas entre un punto de origen y un punto de destino, con la autenticación del origen y la integridad de los datos, hablándose de una asociación de esos datos.

Asimismo, una vez establecida la circulación de la firma electrónica, surge el problema de lo que se puede interpretar como digital en cada país, a la vez que, se fija a ésta el concepto de seguridad y/o la fiabilidad, fundamentándose aspectos como la producción en el sujeto que la emite, la "verificación" de los certificados extranjeros que cumplen los requisitos marcados por la ley y, en el caso de los nacionales, los conocidos por la no muy clara distinción entre lo que es fiable y lo que es seguro.

Por consiguiente, las leyes sobre firma electrónica, en las diferentes jurisdicciones, varían en sus conceptos; incluso cuando se adopta el mismo enfoque, se

pueden detectar diferencias en las disposiciones detalladas con respecto a la naturaleza y la fiabilidad de la firma electrónica, la conducta de las partes y el reconocimiento transfronterizo de las firmas electrónicas y sus certificados, etc.[559].

En este contexto, teniendo en cuenta que los requisitos y normas en conflicto pueden obstaculizar gravemente el reconocimiento de las firmas electrónicas y certificados entre jurisdicciones, lo que nos lleva a estudiar a fondo la interoperabilidad.

4.3.3.1. La interoperabilidad

El término interoperabilidad procede de un vocablo anglosajón y su introducción en el vocabulario técnico, del ámbito de las TIC, se debe a la traducción del término *interoperability*, que ha originado dos posibles alternativas de traducción: interoperatividad o interoperabilidad. Con el paso del tiempo, parece que se ha optado por la preferencia del término interoperabilidad, por dos motivos: uno de orden psicológico, ya que se tiende a adoptar el término en castellano que resulte más parecido al anglosajón; y otro, más determinante, derivado de la elección realizada en las traducciones al castellano de textos de la documentación europea[560], en las que se opta por el término interoperabilidad frente al de interoperatividad[561].

La interoperabilidad es definida, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), como la habilidad de dos o más sistemas o componentes, para intercambiar información y utilizar la información intercambiada[562]; es decir, se trata de

[559] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 144 y ss.
[560] Decisión 1720/1999/CE el Parlamento Europeo y del Consejo de 12 de julio de 1999 sobre un conjunto de orientaciones, entre las que figura la identificación de los proyectos de interés común, relativo a redes transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA).
Disponible en:
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=31999D1720&lg=es (última visita: 30/4/2014).
[561] MARTÍNEZ USERO, M. A.; LARA NAVARRA, P.: *La interoperabilidad de la información, Barcelona*, 2007, págs. 9 y ss.
[562] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: *IEEE Standard Computer Dictionary A Compilation of IEEE Standard Computer Glossaries. Standards coordinatingcodttee of the EEE computer Society*, Nueva York, 1990, pág.113.
Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=182763 (última visita: 30/4/2014).

la capacidad que tiene un sistema para comunicar y funcionar con otro sistema en el intercambio de datos, teniendo en cuenta que, generalmente, se trata de sistemas de diferente tipo, diseñados y producidos por marcas comerciales diferentes.

Tradicionalmente, se han observado tres dimensiones de interoperabilidad: organizativa, relativa a la capacidad de las entidades y de los procesos, a través de los cuales llevan a cabo sus actividades para colaborar con el objeto a alcanzar logros, mutuamente, acordados, relativos a los servicios que prestan; semántica, relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación; y técnica[563], que define los componentes tecnológicos necesarios para lograr el modelo de la interoperabilidad.

A estas dimensiones, se le puede sumar una cuarta: la interoperabilidad jurídica, definida como la sincronización adecuada de la legislación en un ámbito político determinado. En esta dimensión, los datos o documentos electrónicos, que se originan conforme a la legislación de un Estado, deben contar con el reconocimiento legal adecuado, si se quiere que puedan ser utilizados en otro Estado[564].

Dicho de otro modo, la dimensión jurídica de la interoperabilidad consiste en normas, dentro de un determinado sistema jurídico específico, que permita a los actores actuantes en el mercado comunicarse, intercambiar información, ofrecer y usar servicios y productos en tiempo real. Por ello, las normas, que los Estados adopten, deben cumplir con los requisitos marcados en las leyes de los diferentes países o regiones.

---

[563] La interoperabilidad técnica se resuelve, en gran medida, mediante el uso de las normas internacionales aceptadas. En muchos aspectos este problema se resuelve, a través de acuerdos sobre determinadas cuestiones. Un ejemplo, podemos encontrarlo en el Acuerdo firmado por Consejo General de la Abogacía Española y la Federación Argentina de Colegios de Abogados (FACA), integrada actualmente por 82 Colegios de Abogados, por el que ambas abogacías reconocen recíprocamente los certificados digitales de firma electrónica que identifican a sus abogados. La Federación Argentina de Colegios de Abogados, integrada actualmente por 82 Colegios de Abogados, acepta los certificados digitales expedidos por la Abogacía Española, en su calidad de prestador de servicios de certificación. Mientras tanto, el Consejo General de la Abogacía Española reconocerá los certificados que en un futuro se expidan a través de la institución argentina o de sus Colegios asociados. Las Abogacías de España y Argentina cooperarán para garantizar la interoperabilidad de los medios de identificación electrónica. Asimismo y debido al interés recíproco en materia tecnológica, las dos Abogacías acuerdan apoyarse mutuamente, dándose asistencia y asesoramiento, mientras que han expresado su interés en el uso de alguna de las aplicaciones que ambas Abogacías puedan disponer.
Disponible en: http://www.abogacia.es/2014/09/03/las-abogacias-de-espana-y-argentina-reconocen-reciprocamente-la-firma-electronica-de-sus-abogados/ (última visita: 16/9/2014).

[564] GAMERO, E.: "Interoperability and eGovernment: A Legal Approach to the European Union and Spanish Models", *Social Science Computer Review*, 28 febrero de 2011.

A modo de ejemplo, cuando hablamos de interoperabilidad nos estamos refiriendo a que, una autoridad fiscal en un Estado miembro de la Unión Europea, pueda recibir y validar una identidad electrónica emitida por cualquier proveedor de servicios de certificación, establecido en cualquier otro Estado miembro, o de un tercer Estado. Se trata de que, con la información que poseemos, podamos: demostrar la identidad y realizar una transacción jurídicamente vinculante, respetando los requisitos del procedimiento. De este modo, la interoperabilidad se hace posible, con el fin de poder utilizar la misma identificación electrónica en cualquier comunicación nacional o internacional, a través de un procedimiento ya establecido.

De acuerdo con las características de la firma electrónica, que usemos, hablaremos de una forma de promover la interoperabilidad en un ordenamiento jurídico determinado. Hablamos sobre el modelo correspondiente de la interoperabilidad. Diferentes criterios pueden ser utilizados para definir un modelo de interoperabilidad[565]:

a) Voluntarios u obligatorios (vinculantes) en su fuerza: serán voluntarios cuando las organizaciones afectadas (sobre todo las administraciones públicas, implicadas en su ámbito de aplicación) pueden optar por ajustarse a las reglas establecidas u optar por otras soluciones. Por el contrario, serán obligatorios cuando tienen la fuerza para obligar a todas las organizaciones implicadas.

b) Flexibles o rígidos, en su grado de especificidad: en este sentido, las disposiciones relativas a la interoperabilidad pueden ser absolutamente rígidas (por ejemplo, cuando imponen el requisito de que todas las administraciones públicas deben aceptar una firma electrónica específica, como un documento nacional de identidad electrónico) o flexibles,

[565] En la práctica, hay modelos de interoperabilidad que corresponden a diferentes combinaciones de las categorías anteriores. Por ejemplo, el modelo tradicional de la Unión Europea es voluntario, flexible, unitario y participativo. En general, ha habido una transición de modelos de interoperabilidad voluntarios, flexibles, descentralizados y unilaterales y hacia la introducción de modelos interoperabilidad obligatorios, rígidos, unitarios y participativos. Esta es una transición inevitable en un mundo que se está volviendo cada vez más interconectado.

refiriéndose simplemente a las normas generales, fuentes abiertas u otras categorías que unen un margen de actuación a los diferentes operadores.

c) Unitarios o descentralizado: tal como fue aprobado por una autoridad que proyecta su influencia y su valor vinculante a los demás (por ejemplo, la Unión Europea a los Estados miembros, una federación en sus Estados federados, el Estado en las regiones o Comunidades autónomas) o adoptado por medio de la cooperación (o instrumentos de cooperación), entre las diferentes instituciones en posiciones iguales.

d) Participativos o unilaterales: atendiendo a como se han utilizado en el proceso de elaboración de técnicas o en el uso de los enfoques.

Ante la situación descrita, observamos que el problema deriva de la falta de neutralidad tecnológica; pues, los procesos, tecnologías y protocolos requeridos, para asegurar la integridad de los datos, cuando se transfieren de un sistema a otro, deberan conllevar, por definición, una correcta interconexión de los sistemas e intercambio de datos.

En efecto, algunos sistemas jurídicos, como sabemos, se basan en la neutralidad tecnológica, lo que significa que los ciudadanos tienen el derecho a elegir las soluciones técnicas, que quieran utilizar en los campos nacionales y en las relaciones que mantienen con la administración pública. En consecuencia, la administración pública, al imponer una tecnología concreta, reduce el derecho a elegir; por ejemplo, la situación legal en España.

Así, en el plano técnico, aunque abundan las normas, se ha de poner de relieve la falta de normas básicas comunes a algunas tecnologías. En el plano jurídico, las legislaciones, que prescriben una tecnología específica predominante, se señalan como factores, que impiden el progreso, la dificultad de los responsables en comprender sus

respectivos marcos de confianza mutua e incluso en los temas de responsabilidad e indemnización[566].

Como resultado de esta situación, las empresas y particulares se ven obligados a mantener más de un sistema para la realización de una tarea, resultando ésta ardua y difícil, a la hora de extraer toda la información necesaria, por encontrarse en aplicaciones aisladas[567], algo que tiene mucho que ver con la falta de neutralidad tecnológica.

Teniendo en cuenta la situación planteada, el Grupo de Trabajo de la OCDE[568], señaló puntos a analizar, con el fin de elaborar instrumentos comunes en los distintos ordenamientos jurídicos, abordando cuestiones como: el desarrollo (por ejemplo, directrices, mejores prácticas, plantillas para el desarrollo de los acuerdos) para facilitar la interoperabilidad, incluidos los aspectos relacionados con la aceptación de servicios extranjeros y los certificados y la aceptación de credenciales de los otros proveedores de servicios; el desarrollo de un marco, para evaluar los atributos de métodos de autenticación, para que puedan ser evaluados en cuanto al grado de satisfacción de los requisitos de una aplicación particular; el desarrollo de principios prácticos de información al entorno de autenticación; desarrollar iniciativas orientadas a definir el modelo de negocio para la autenticación, en estrecha cooperación con y en base a las aportaciones del sector privado.

Como puede observarse, el Grupo de Trabajo de la OCDE[569] señaló como gran escoyo la interoperabilidad, que deriva de la falta de reconocimiento de los servicios de certificación ante la gran variedad de métodos de autenticación. Así pues, resulta importante la estructura interna de cada organización; pues, ésta va a condicionar la interoperabilidad en el intercambio de datos, información o conocimiento con otras

[566] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005, pág. 6.
[567] Disponible en: www.abartiateam.com/interoperatibilidad (última visita: 2/5/2014).
[568] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005, pág. 7.
[569] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005, pág. 6.

organizaciones, que posean una estructura interna diferente; lo que viene a relacionarse con la reglamentación de distintos tipos de firma electrónica, en referencia a los distintos grados de seguridad con que cuenta y, especialmente, si se presta énfasis regulatorio sólo a uno de ellos, resultando las normas existentes un obstáculo para la interoperabilidad, por el establecimiento de requisitos añadidos.

Un ejemplo, al problema de la interoperabilidad es la situación que está presente en el ámbito de la Unión Europea: las autoridades estatales de toda Europa han empezado a ofrecer acceso electrónico, centrándose, sobre todo, en las necesidades y medios nacionales, lo que ha generado un sistema complejo con soluciones diferentes, que ha provocado el nacimiento de nuevos obstáculos a los intercambios transfronterizos, que lastran el funcionamiento del mercado único para las empresas y los ciudadanos. Así, la Comisión reconoce lo necesaria que es la interoperabilidad efectiva, para que las empresas puedan ejercer sus derechos y realizar transacciones a través de las fronteras[570].

La falta de interoperabilidad es principalmente dada por la obligación impuesta a los proveedores de servicios de certificación, que al expedir certificados reconocido,s en cumplimiento del Anexo II de la Directiva 1999/93/CE sobre firma electrónica, deben: "comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido".

Atendiendo a lo comentado anteriormente, si queremos realizar una transacción transfronteriza con el certificado emitido; por un lado, tenemos, que los documentos de identificación electrónica son dependientes de un documento de origen y la integridad de un sistema de identificación depende de una relación demostrable entre la persona y el prestador de servicios, que emite el certificado con el que se va a firmar el documento en el mismo país de origen; por otro, surgirá la necesidad demostrar la identidad y realizar la autenticación de la transacción jurídicamente vinculante, en el país de

[570] COMISIÓN EURPEA: *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM (2008) 798 final): sobre el Plan de acción de sobre firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único,* Bruselas, 28 de Noviembre de 2008.

destino, lo que nos exige respetar los requisitos del procedimiento establecido por este Estado, lo que perjudica gravemente a la interoperabilidad.

El camino[571] de una posible solución se marca a través del Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, que reconoce que la interoperabilidad y el reconocimiento transfronterizo de los certificados cualificados son requisitos previos, para el reconocimiento transfronterizo de las firmas electrónicas cualificadas. Por consiguiente, los certificados cualificados no deben estar sometidos a ningún requisito obligatorio, que exceda de los requisitos establecidos en el presente Reglamento. No obstante, en el plano nacional debe permitirse la inclusión de atributos específicos; por ejemplo, identificadores únicos, en los certificados cualificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizo de los certificados y las firmas electrónicas cualificados[572].

Esto se viene a realizar a través de la evaluación exhaustiva de una serie de aspectos en la emisión del certificado[573]: a) la documentación que se tiene que presentar al proveedor de servicios de certificación; b) los requisitos procedimentales que son

[571] Ante la fragmentación de los mercados digitales y la falta de interoperabilidad, la Comisión Europea desarrolló: medidas de impulso de la firma electrónica en el ámbito de los servicios transfronterizos dentro de la Unión Europea (COMISIÓN EUROPEA: *Comunicación, de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, titulada "Agenda digital para Europa" (COM (2010) 245 final)*, Bruselas, 19 de mayo de 2010.); propuestas con el fin de avanzar hacia un mercado único digital, considerando la posibilidad de disponer de una "legislación que garantice el reconocimiento mutuo de la identificación y autentificación electrónicas en toda la UE y revisión de la Directiva sobre la firma electrónica. El objetivo es conseguir una interacción electrónica segura y sin obstáculos entre empresas, ciudadanos y administraciones públicas para aumentar, incluso en su dimensión transfronteriza, la eficacia de los servicios, de los contratos públicos, de la prestación de servicios y del comercio electrónico" (COMISIÓN EUROPEA*: Comunicación de la Comisión al Parlamento, al Consejo, al Comité Económico y Social y al Comité de las Regiones: Acta del Mercado Único Doce para impulsar el crecimiento y reforzar la confianza "Juntos por un nuevo crecimiento* , Bruselas, 27 de octubre de 2011 (COM (2011) 206), pág. 14); así como una Hoja de ruta para la estabilidad y el crecimiento en la que se da prioridad a las propuestas recogidas en el Acta del Mercado Único, especialmente a una base jurídica común para el reconocimiento mutuo de la autenticación y la firma electrónicas más allá de las fronteras nacionales COMISIÓN EUROPEA*: Comunicación de la Comisión: Hoja de ruta para la estabilidad y el crecimiento*, Bruselas, 12 de octubre de 2011, págs. 6 y 7).

[572] Considerando 54 del Reglamento 910/2014 relativo a a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

[573] Artículo 24 del Reglamento 910/2014 relativo a a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

obligatorios; c) cuáles son las exigencias de prueba de la identidad; d) cuál es la información que tiene que estar en el certificado para demostrar una identidad y cómo se va a presentar a una contraparte; y e) cómo puede la contraparte verificar la información de la identificación electrónica, para poder establecer la conexión entre la persona física y el titular declarado de la identificación electrónica.

De esta forma, se viene fijar a la implantación de los medios técnicos necesarios para procesar los documentos firmados electrónicamente, para que los prestadores de servicios puedan llevar a cabo sus procedimientos y trámites por vía electrónica a través de las fronteras, lo que hace necesario garantizar, que los Estados miembros, puedan dar soporte técnico, al menos, a cierto número de formatos de firma electrónica avanzada, cuando reciban documentos firmados electrónicamente por autoridades competentes de otros Estados miembros.

De este modo, se puede concluir que, en los respectivos marcos de confianza, que se regulan en las Leyes nacionales, incluyendo la asignación de responsabilidad, son parámetros que necesitan ser desarrollados con vistas, a la trasposición del mencionado Reglamento, con el fin de establecer herramientas comunes, que permitan ayudar a las distintas jurisdicciones a lograr el nivel de interoperabilidad deseado, bien para una aplicación, bien para un sistema en particular.

A día de hoy, todos los enfoques centran sus esfuerzos en el establecimiento de servicios de certificación de carácter nacional, no desarrollando de forma adecuada los servicios de autenticación extranjeros, a lo que hay que sumar el establecimiento de requisitos añadidos, que se refieren de manera expresa al reconocimiento de certificados extranjero, lo que nos permite hablar en la práctica de sistemas cerrados, ya que los titulares de los certificados quedan estrechamente vinculados por reglas preestablecidas, que vienen a describir, de forma más precisa, los fines para los que pueden utilizarse los certificados u otra información de autenticación electrónica.

Así, la divergencia normativa internacional nos muestra una combinación de factores, que nos hace ver la interoperabilidad como uno de los obstáculos principales de las firmas y autenticación electrónica:

a) Países que tienden a establecer unos criterios más estrictos y particularizados, en lo que respecta a las firmas y documentos.

b) Otros se centran en la intención del firmante y permiten una extensa variedad de formas de probar la validez de las firmas electrónicas.

c) Y, por último, otros se centran en la injerencia de las autoridades nacionales en los aspectos técnicos de dichos métodos.

Un marco que parece haber superado la prueba de interoperabilidad, a la espera de cómo transcurre la aplicación directa del Reglamento europeo, es: Identrus, red que utiliza las relaciones bancarias establecidas para permitir, a las empresas, autenticar las transacciones con otras empresas, lo que les permite asignar claramente el riesgo y la responsabilidad.

CAPÍTULO QUINTO: INTERNACIONALIZACIÓN DE LA FIRMA ELECTRÓNICA

5.1. Introducción

Ante la posibilidad de proyectar la firma electrónica en una transacción internacional, nos podemos encontrar con un problema de validez; es decir, ante el riesgo de que un Tribunal se niegue a admitir nuestra firma electrónica por diferencias latentes en las Leyes que imperan en la transacción[574].

Una pregunta clave que debemos hacernos, antes de iniciar una transacción con carácter transfronterizo, es si: ¿es posible dar el consentimiento a través de una transacción electrónica, mediante el uso de una firma electrónica? Si es así, ¿se asegura la aplicabilidad de esa firma electrónica en un país extranjero? Estas preguntas son problemas recurrentes, que si bien podría resultar un simple problema doctrinal, es algo que se produce en la práctica y plantea dificultades, para las empresas que buscan poder asegurar la exigibilidad de sus contratos más importantes.

Ante esta situación se debe establecer una regla de interpretación de la Ley. Ésta habrá de interpretarse en conjunto con el resto del ordenamiento, para determinar cuál es la intención legislativa de la que se debe de partir[575].

Las leyes estatales están destinadas a desarrollar un marco normativo capaz de hacer frente a la legalidad y aplicabilidad de las firmas electrónicas. Sin embargo, el reconocimiento de la firma electrónica es un tema importante en el que, los distintos Estados, no han sido capaces de ponerse de acuerdo a la hora de establecer un enfoque uniforme en el desarrollo de las leyes de firma electrónica. La aceptación del formato de

[574] SCHAPPER, P.R.; RIVOLTA, M.; VEIGA, J.: "Risk and law in authentication", *Digital evidence and electronic signature law review*, octubre, 2006, núm. 6, págs. 12- 18.
[575] ESTADOS UNIDOS: Vista Developers Corp. V. VFP Realty LLC, 2007, NY Slip Op 27418 (17 Misc. 3d 914) Supreme Court, Queens County, 8 octubre de 2007.
Disponible en: http://www.courts.state.ny.us/Reporter/3dseries/2007/2007_27418.htm última visita, 11-3-2014).

la firma electrónica ha quedado al arbitrio de cada país[576], lo que nos lleva al riesgo de que el Tribunal de un país determinado se niegue a admitir como prueba un documento electrónico firmado.

Cierto es que cualquier persona física o jurídica o, incluso, una administración de cualquier país, en el curso normal de su negocio o actividad, firma electrónicamente documentos en el acto de cualquier transacción necesaria, para el desarrollo de su actividad o negocio, teniendo que hacer valer la firma electrónica, con la que se han identificado ante las leyes sustantivas de otros países, que obligan a que se cumplan determinadas características, para evitar la discriminación de la información contenida en el documento electrónico.

Todas las legislaciones mundiales, sobre firma electrónica, han partido de unos denominadores comunes, que hoy en día no se discuten:

a) La aceptación del formato electrónico como equivalente del escrito, es decir, el principio de equivalencia funcional, entendiendo por éste la función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa, respecto de cualquier acto jurídico, igualmente, su instrumentación electrónica a través de un mensaje de datos con independencia del contenido, dimensión y finalidad del acto[577]. De esta manera, tratan de darle a las firmas electrónicas un papel equivalente al dado a la firma manuscrita, con el fin de darle confianza en la lucha contra el fraude[578].

b) La inalterabilidad del derecho preexistente, la contratación a distancia ha sido recogida en los ordenamientos jurídicos de todo el mundo, al regular la contratación vía telegrama o carta. En esto se acogen todos los ordenamientos jurídicos, que con las nuevas tecnologías no alteran las reglas

[576] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE* (2001), párr. 5.
[577] ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 39.
[578] UNCITRAL/CNUDMI: *Recognizing and Preventing Commercial Fraud, Indicators of Commercial Fraud*, Nueva York, 2013, págs.70 y ss.

> generales de la contratación en lo que respecta a los contratos, de tal manera que no exigen ningún requisito particular de forma, sino que solo crean un medio para su celebración; es decir, como dice el Prof. Illescas, no es necesario ni conveniente confeccionar íntegramente un sistema de derecho contractual para los negocios electrónicos, sino que basta con mantener las excepciones de libertad de forma más relevantes[579].

Se trata de principios, que se han desarrollado internacionalmente, sobre la contratación electrónica, a través del trabajo incesante, entre otros, por la CNUDMI/UNCITRAL[580], sin que se hayan llegado a imponer a los Estados, lo que ha llevado a que, la aceptación del formato electrónico como equivalente del escrito, se haya quedado al arbitrio de cada país[581].

De esta suerte, el problema de fondo que nos encontraremos[582], con el análisis de las firmas electrónicas reguladas en las distintas legislaciones examinadas, se puede concretar, en nuestra opinión, en la siguiente afirmación: la fuerza y validez de la firma electrónica transfronteriza va a depender de que se consiga el objetivo de dar confianza a la transacción que se realiza, quedando supeditado al tipo de firma electrónica que se utilice, permaneciendo latente en el pulso que mantienen la fiabilidad frente a la seguridad.

Sabemos que firmas electrónicas hay de muchos tipos[583], tantas como formas de creación hay. Uno de los primeros formatos de firmas electrónicas fue la basada en el EDI (*Electronic Data Interchance*), que surgió en los años 80, siendo, a día de hoy, una de las más consolidadas.

---

[579] ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 49 y ss.
[580] MADRID PARRA, A: "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista de Derecho Patrimonial*, año 2003 – 2, número 11, págs. 31 - 63.
[581] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 145.
[582] ESTRELLA-FARIA, J.A.: "Legal Aspects of Electronic Commerce in International Trade (Part II) – Electronic Authentication and Signature Methods: Legal Issues and Public Policy", *CNUDMI: Recursos en línea y transmisiones web*.
Disponible en: http://legal.un.org/avl/ls/Estrella-Faria_IEL_video_2.html (última visita: 14/3/2014).
[583] FORDER, J.: "The inadequate legislative response to e-signatures", *Computer Law and Security Review*, Julio, 2010, Vol. 26, núm. 4, págs. 418 – 426.

En su vertiente comercial, EDI consiste en la realización de transacciones comerciales de forma automatizada, con el intercambio, en formato normalizado, de órdenes de compra, dentro de comunicaciones sectoriales y, generalmente, a través de redes cerradas cuyo uso, previo pago, es proporcionado por los correspondientes proveedores de servicios. Las transacciones tradicionales vía EDI requieren, generalmente, una fase de preparación y negociación entre las partes implicadas, para establecer los protocolos técnicos y administrativos que les serán aplicables. Por ello, implica la existencia de relaciones comerciales duraderas, a largo plazo, con cierto volumen de operaciones, entre partes próximas, que son empresas mutuas y recíprocamente conocidas y dignas de confianza; pues, sólo este tipo de relación justificaba los altos costes de puesta en funcionamiento de EDI[584].

Los formatos más simples de firma electrónica[585] pueden ser, por ejemplo: un nombre escrito en la parte inferior de un correo electrónico, un clic en el botón "Acepto" en un sitio web o el escaneo de firmas manuscritas. Estos tipos de firmas son consideradas, por muchas legislaciones, inseguras, por ser incapaces de garantizar la identidad del remitente, así como la integridad del documento.

Otra forma de las firmas electrónicas son las firmas digitales, un tipo de firma electrónica que utiliza tecnología de cifrado seguro conocido como la infraestructura de clave pública (PKI)[586], que proporcionan autenticidad, integridad y no rechazo en origen del mensaje de datos. La firma digital necesita de una entidad certificadora que asegure, entre otras muchas funciones, el vínculo entre la clave pública y el titular de la clave privada. Dada la naturaleza transfronteriza del comercio electrónico, con las firmas digitales, se presentan, esencialmente, dos problemas: por un lado, que sean válidas e interoperables entre los diversos países a través del reconocimiento internacional de certificados; por otro, respecto de las entidades certificadoras, se plantea la delimitación de riesgos, derechos, deberes, obligaciones y responsabilidades por la emisión de certificados en el uso internacional.

---

[584] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 29 y ss.

[585] NORTON, W. K.: "Enforcing 'simple' electronic signatures in an international context", Digital *evidence and electronic signature law review*, octubre, 2012, núm. 9, págs.74 – 78.

[586] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 41 y ss.

Cada uno de los distintos tipos de firma electrónica obedecen al objeto de atender a las distintas necesidades, que se ofrecen ante los diferentes tipos de transacciones electrónicas, que se pueden presentar internacionalmente[587], ya sea entre empresas, empresa y consumidor, entre consumidores, entre consumidor y administración o entre empresa y administración.

Algunos países han optado por una firma electrónica tecnológicamente neutral, haciendo referencia a todos los métodos por los que se puede firmar electrónicamente. En otros casos, se ha optado por marcos normativos a favor de una tecnología específica, especialmente, la tecnología PKI, y, en otros casos, se ha optado por el establecimiento de un enfoque intermedio.

La falta de uniformidad y diferencias en las legislaciones han dado lugar a un enfoque incoherente, así como a un debate significativo con respecto a la trascendencia jurídica de la firma electrónica[588].

La actividad legislativa sobre firma electrónica se ha venido desarrollando sobre el interrogante de su validez y su eficacia, sobre la base del derecho nacional existente y no sobre su validez en la transacción internacional. Así, el riesgo de admisibilidad de la firma electrónica nos lleva a la proyección del principio de no discriminación y éste, a su vez, a la más que necesaria coordinación internacional.

5.2. Reconocimiento transfronterizo de la firma electrónica simple

Hemos observado, que todas las empresas a las que hemos consultado, muestran un gran interés en las ventajas que les ofrecen las comunicaciones electrónicas para celebrar contratos con otras empresas, consumidores y administraciones de todo el mundo.

[587] CRUZ RIVERO, D. "Contratación electrónica con consumidores", *Revista de la contratación electrónica*, Nº 109, 2009, p. 3 – 42.
[588] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 145.

Por este motivo, se muestran interesadas en encontrar algún formato que les permita asegurar la exigibilidad del contrato que se firma electrónicamente y, a la vez, muestren la identidad del firmante, sin que esto afecte al proceso negociador; es decir, tratan de buscar un marco de confianza mutua atendiendo a las necesidades y posibilidades del cliente, evitando incrementar las posibles cargas que puedan darse en los procesos de negocio.

Las empresas, por supuesto, saben de la existencia de las firmas electrónicas avanzadas, reconocidas, seguras, cualificadas o digitales, que se han desarrollado con un trato claramente preferencial, en casi todos los países[589]; pero, son conscientes de lo difícil y costoso que resulta satisfacer la tecnología requerida, cuando se trata de un país distinto al suyo. Así pues, ante la complejidad existente cuando se trata del uso internacional de esta firma electrónica, las empresas intentan interactuar a través del uso de la firma electrónica simple.

De esta forma, tratan de adaptar sus procesos de contratación, con el fin de hacer valer las firmas electrónicas simples, en lugar de coordinar el uso de firmas digitales con sus clientes y socios. Sin embargo, el uso internacional de la firma electrónica simple puede resultar problemático, por el diferente trato que se le ha dado a ésta en todos los Estados.

5.2.1. Reconocimiento normativo

Todas las leyes sobre firma electrónica comienzan con una definición de firma electrónica neutral tecnológicamente. Fijémonos, en primer lugar, como no puede ser de otra manera, en lo que se entiende por firma electrónica simple en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, sobre firma electrónica, tal y como se recoge en el Artículo 2,1: "A efectos de la presente Directiva, se entenderá por: 1) firma electrónica: los datos en forma electrónica anejos a

[589] NORTON, W. K.: "Enforcing 'simple' electronic signatures in an international context", *Digital evidence and electronic signature law review*, octubre, 2012, núm. 9, págs.74 – 78.

otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación"[590].

Como comenta la Prof. Martínez Nadal[591], la Directiva muestra la neutralidad tecnológica de forma conveniente, podría decirse que lo hace para dejar abiertas las puertas a los posibles desarrollos tecnológicos, pero lo hace llevando la normativa al extremo; pues, como se puede ver, deja sin resolver las cuestiones relativas a su validez y eficacia, porque ni siquiera son abordadas en el conjunto de la regulación, al centrarse, en exclusiva, en las firmas digitales, lo mismo pasa en la transposición que llevan a cabo los Estados miembros.

Para evitar un posible resultado restrictivo y excluyente, se establece una cláusula de salvaguarda en el Artículo 5,2, que nos dice que los Estados miembros velarán porque no se niegue eficacia jurídica, ni la admisibilidad, como prueba en los procedimientos judiciales, a la firma electrónica por el mero hecho de que: ésta se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o no esté creado por un dispositivo seguro de creación. Este Artículo se ha recogido en todas las legislaciones europeas.

Esta cláusula de salvaguarda[592] tiene sentido ante la clara discriminación normativa existente entre los tipos de firma electrónica recogidos en la Directiva: la firma electrónica simple, avanzada y la reconocida. Hay grandes diferencias entre ellas, si bien este tema no se reconoce de manera explícita, está claro que la mayoría de los comentarios que se recoge en las legislaciones, estudios, libros, etc. se refieren específicamente a las firmas basadas en certificados reconocidos; es decir, las firmas avanzadas basadas en certificados reconocidos y certificados cualificados.

---

[590] En el Reglamento Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, en el Artículo 2,10) define la firma electrónica como "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar"; aunque ambas difieren en su concepción final, mantienen el trato tecnológico.

[591] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 54 y ss.

[592] TAUBER, A; KUSTOR, P.; KAMING, B.: "Cross-border certified electronic mailing: A European perspective", *Computer Law and Security Review*, Vol. 29, núm. 1, febrero, 2013, págs.28 – 39.

Con esta cláusula, en nuestra opinión, se trata de asegurar que las incertidumbres legales, que rodean el valor de la firma electrónica, no se conviertan en una barrera para el incipiente mercado de la firma electrónica en la Unión Europea; o sea, de que tales incertidumbres sean mínimas. La eliminación de todo tipo de inseguridad jurídica es complicada, debido a la gran variedad de enfoques existentes para las firmas electrónicas y sus características técnicas. El legislador europeo tenía que trazar una línea muy fina entre la flexibilidad, permitiendo diferentes tecnologías con diferentes grados de fiabilidad, y la seguridad jurídica, garantizar la previsibilidad del valor jurídico de, al menos, algunos tipos de firma electrónica[593].

Asimismo, se observa que cuando la Directiva establece lo que debe entenderse por firma electrónica simple, está relacionando este tipo de firma implícitamente y en sentido contrario, con la firma electrónica reconocida; es decir, con el concepto de seguridad[594]. Por este motivo, no puede decirse que se dé una definición de firma electrónica, sino una relación de elementos de lo que debe entenderse por firma electrónica simple respecto a la seguridad que viene de la firma electrónica reconocida, considerada como equivalente a la firma manuscrita.

El modelo de confianza actual de la Directiva, que se traslada a los Estados miembros, está sustancialmente relacionada con este concepto: la confianza en las firmas puede ser determinada por el hecho de que los certificados cualificados comparten necesidades comunes (Anexo I de la Directiva) , al igual que los Prestadores de Servicios de Certificación que expiden estos certificados al público (Anexo II de la Directiva), el cumplimiento es supervisado por órganos de control específicos con un mandato nacional, en virtud del Artículo 3,3, lo que supone que el modelo de firma electrónica simple se relacione de forma inmediata con la seguridad.

Teniendo en cuenta lo dicho anteriormente, cuando hablamos de la firma electrónica simple, con la Directiva en la mano, debemos observar el posible origen de este precepto, que quizá pueda situarse en la proximidad legislativa de Reino Unido.

[593] MANSON, S.: *Electronic signature in Law*, Cambridge, 2011, págs. 115 y ss.
[594] MANSON, S.: *Electronic signature in Law*, Cambridge, 2011, págs. 154 y ss.

Por ello, veamos el trato dado por Reino Unido a la Directiva. Reino Unido recoge la firma electrónica simple en el Artículo 7,2 de la *Electronic Communications Act*[595], como algo que está en forma electrónica y que: a) se incorpora o asocia lógicamente a cualquier comunicación electrónica o mensaje electrónico de datos; y b) pretende estar incorporado o asociado con el propósito de ser utilizado en el establecimiento de la autenticidad de la comunicación o los datos, la integridad de la comunicación o de datos, o ambos[596]. Además, se requiere que ha de haber una declaración hecha por una persona (ya sea antes o después de la realización de la Comunicación) que confirme que la firma, el medio de producción, comunicación o verificación de la firma o que el procedimiento que se aplica a la firma es un medio válido para establecer la autenticidad de la comunicación o los datos, la integridad de la comunicación o de lo datos, o de ambos. Asimismo, la Ley recoge expresamente su admisibilidad como prueba, pues viene a decir que: será admisible como tal si la firma electrónica se fija a los datos para autenticar la comunicación o para proporcionar su identidad a la comunicación o a los datos[597].

[595] Electronic Signatures Regulations 2002 (SI 318/2002): Secc. 7.- Electronic signatures and related certificates.
"(1) In any legal proceedings:
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
(b) The certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.
(2) For the purposes of this section an electronic signature is so much of anything in electronic form as:
(a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
(b) Purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.
(3)For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that:
(a) the signature,
(b) a means of producing, communicating or verifying the signature, or
(c) A procedure applied to the signature, is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both".
[596] HEDLEY, S.: *The Law of electronic commerce and the internet in the UK and Ireland*, Londres, 2006, págs. 250 y ss.
Disponible en: http://www.legislation.gov.uk/ukpga/2000/7/contents (última visita: 19/3/2014).
[597] MANSON, S.: *Electronic signature in Law*, Cambridge, 2011, pág.143 y ss.

En otras palabras, la firma electrónica se define como cualquier medio de autenticación electrónica de la identidad de una persona y de la intención de esa persona para indicar la aprobación o estar asociado con un registro electrónico[598].

El Artículo 8 de la Ley[599] otorga amplios poderes al Gobierno para autorizar o facilitar las comunicaciones electrónicas, mediante la eliminación de las restricciones que puedan venir derivadas de las disposiciones de la Ley, impidiendo el uso de las comunicaciones electrónicas. Este poder puede ser utilizado incluso de forma selectiva para ofrecer una alternativa electrónica a quiénes lo deseen.

Con todo lo anterior, se aprecia que la *Electronic Communications Act* establece un marco regulatorio tecnológicamente neutral, con una definición de firma electrónica diferente en cuanto a sus elementos y adoptando sólo algunas disposiciones de la Directiva. Esta neutralidad se rompe con la *Electronic Signatures Regulations* (SI 318/2002), aprobada en 2002, que aunque tarde, pues la regulación contenida en esta norma debería haber sido adoptadas antes del 19 de julio de 2001, viene a establecer las disposiciones necesarias para dar cumplimiento a las disposiciones legales recogidas en la Directiva 1999/93/CE sobre firma electrónica

[598] DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009, pág. 81.

[599] Electronic Signatures Regulations 2002 (SI 318/2002): "Secc. 8.- Power to modify legislation:
(1)Subject to subsection (3), the appropriate Minister may by order made by statutory instrument modify the provisions of:
(a) any enactment or subordinate legislation, or
(b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation, in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).
(2)Those purposes are:
(a)the doing of anything which under any such provisions is required to be or may be done or evidenced in writing or otherwise using a document, notice or instrument;
(b)the doing of anything which under any such provisions is required to be or may be done by post or other specified means of delivery;
(c)the doing of anything which under any such provisions is required to be or may be authorised by a person's signature or seal, or is required to be delivered as a deed or witnessed;
(d)the making of any statement or declaration which under any such provisions is required to be made under oath or to be contained in a statutory declaration;
(e)the keeping, maintenance or preservation, for the purposes or in pursuance of any such provisions, of any account, record, notice, instrument or other document;
(f)the provision, production or publication under any such provisions of any information or other matter;
(g)the making of any payment that is required to be or may be made under any such provisions".

Con este marco reglamentario, Reino Unido recoge el resto de disposiciones exigidas por la norma comunitaria. De esta forma, se observa como el ordenamiento jurídico inglés parece recoger los distintos niveles de firma electrónica, pero mediante una regulación separada entre ellas, aunque íntimamente conectadas.

Este hecho nos hace ver que el legislador inglés opta por el principio de neutralidad tecnológica como eje de una forma clara e inequívoca y, con ello, prevé el reconocimiento legal de la firma electrónica con independencia de la tecnología utilizada para su creación. Así, establece que una firma electrónica es una prueba admisible en cuanto a la autenticidad del mensaje o su integridad. Además, corresponderá a los Tribunales decidir en cada caso particular, si una firma electrónica ha sido utilizada correctamente y qué peso se le debe dar (por ejemplo, en relación con la autenticación o la integridad de un mensaje) contra otras pruebas, lo que podría suponer, situar a la firma electrónica en una posición de debilidad extrema[600].

En Reino Unido no hay requerimientos formales para las transacciones comerciales y, obviamente, si por ejemplo, un contrato oral puede considerarse válidamente hecho, no hay razón para que un contrato no pueda ser concluido usando cualquier medio electrónico. Siempre ha habido un enfoque flexible para la aceptación de las nuevas tecnologías. Así, grabados[601], sellos de caucho[602], mecanografías[603] y telegramas[604] han llegado a satisfacer los requisitos de firma en determinadas circunstancias.

Asimismo, con los amplios poderes concedidos al gobierno en el Artículo 8 se hace más fácil hacer frente a los problemas que pudieran surgir, pero no ofrecen claridad; pues, podrían invalidar los requisitos ya establecidos[605]. En este escenario, se deja el asunto al Juez, que si efectivamente actúa de una forma flexible, no habrá nada que impida el reconocimiento de diversos métodos de firma electrónica simple.

[600] DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009, pág. 91 y ss.
[601] REINO UNIDO: Bennet v Brumfitt (1867-1868) 3 LRCP 28.
[602] REINO UNIDO: Jenkins v Gaisford y Thring (1863) 3 Sw & T 93.
[603] REINO UNIDO: Godwin v Francis (1870) LR 5 CP 295.
[604] REINO UNIDO: Newborne v Sensolid (Gran Bretaña) LD [1954] 1 QB 45.
[605] FORDER, J.: "The inadequate legislative response to e-signatures", *Computer Law and Security Review*, Julio, 2010, Vol. 26, núm. 4, págs. 418 – 426.

Llegado a este punto, observemos la definición por la *Electronic Signatures in Global and National Commerce Act* (E-Sign), de Estados Unidos, que, en la Sec. 106, recoge la definición de firma electrónica como: *The term ''electronic signature'' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.*

Observamos que es, claramente, abierta al considera como firma electrónica cualquier medio electrónico de autenticación de datos, con independencia de su seguridad en un ulterior proceso probatorio. La firma es un requisito inherente al documento; es decir, es un gesto que, plasmado en el documento, muestra que asume la declaración contenida en el mismo[606]. Postura similar a la adoptada por Reino Unido en la *Electronic Communications Act*.

Este criterio definitorio adoptado, es el estándar que, como regla general, se ha establecido en los países de la *common law*. De esta forma, hemos observado que han establecido en sus ordenamientos jurídicos que la forma de la firma es lo menos importante; o sea, lo que verdaderamente importa es la intención que hay detrás de la firma, para formar un documento jurídico vinculante.

Con ello, se alienta a los Tribunales para que interpreten la Ley, estableciendo por firma electrónica cualquier método de comunicación intangible, capaz de identificar a la persona que almacena, transmite y reproduce la información; de la misma manera que se trata de alentar en su conjunto al mercado e individualmente a cada persona a la elección de la tecnología o método adecuado a sus necesidades, sin dejar de prestar atención a una estructura ya preestablecida.

5.2.2. Validez y eficacia normativa

La mayoría de las Leyes, dependiendo de un país u otro, especialmente en los países de la Unión Europea, consideran la seguridad de la firma electrónica para juzgar

[606] WANG, M: Do the regulations on electronic signatures facilitate international electronic commerce? A critical review, *Computer Law and Security Review*, 2007, Vol. 23, núm. 1, págs. 32 – 41.

la fiabilidad del sistema[607]. Esto significa que una firma no es mejor por su calidad sino por la confianza (entendiendo confianza en términos de seguridad), que es capaz de crear dentro del sistema en el que se encuentra; pues, la prueba de la integridad de un documento electrónico requiere una prueba de la integridad del sistema de firma electrónica, instaurado en la Ley del país de destino[608].

Por tanto, para que una firma electrónica esté en condiciones de generar un valor jurídico indubitable, de tal manera que sea aceptada en los procedimientos legales, en el sistema de gestión dentro del país en el que opera, debe cumplir con las especificaciones que marca por la Ley. Cualquier cambio que se realice en un sistema, afecta al propio sistema y, por tanto, a su nivel de rendimiento[609].

Por consiguiente, siempre que el firmante se mantenga dentro de un contexto específico, como puede ser: las aplicaciones de banca electrónica, los servicios nacionales de gobierno electrónico, los sistemas de gestión de documentos profesionales, etc. dentro de un país concreto, se puede observar el marco establecido sin problema y, dentro de este marco, pueden establecerse soluciones para cualquier tipo de cuestión. Pero en cuanto se trata de utilizar una firma digital fuera de ese marco establecido, las firmas electrónicas digitales parecen quedar sin uso.

Lo que nos lleva a pensar que, si a la hora de otorgar validez a una firma electrónica se hiciera depender de que ésta sea tan fiable como apropiada a las circunstancias de cada caso en concreto, no se daría discriminación alguna.

Esta parece ser la postura adoptada en los países de la *common law*[610] donde a la firma electrónica no se le imponen requisitos de forma en el establecimiento de lo que puede ser una firma; por tanto, no se necesita ninguna norma legal más para enfatizar el apoyo de una firma electrónica, es decir, las Leyes de la firma en los países de la *common law* enfatizan la función de la firma sobre la forma, en contraste con los países

[607] KRAWCZYK, P.: "When the EU qualified electronic signature becomes an information services preventer", *Digital evidence and electronic signature law review*, octubre, 2010, NÚM. 7, págs. 7 – 18.
[608] BRAZEL, L: *Electronic Signatures, Law and Regulation*, Oxford, p. 45 y ss.
[609] GREGORY, J.D.: "Must e-signature be reliable?" *Digital evidence and electronic signature law review*, octubre, 2013, núm. 10, págs. 67 – 70.
[610] SIMMONS & SIMMONS: *E-Commerce Law: doing business online*, Bembridge, pág. 31 y ss.

de la *civil law*, que hacen hincapié de la forma sobre la función, haciendo necesario considerar, la base de la normativa sobre firma electrónica, en el uso de una tecnología; es decir, en la tecnología digital[611].

La postura adoptada en Europa, por la Directiva y ahora por el Reglamento, lleva al extremo máximo el criterio adoptado en Ley Modelo de Comercio Electrónico, que viene a decir en su Artículo 7, respecto a la firma: "Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos... b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente".

Esto supone decir que, cualquier requisito legal, en relación con el proceso de firma electrónica, debe ser tan fiable como sea apropiado a las circunstancias; o sea, impone un criterio de seguridad[612]. Dicho en sentido contrario, no impone un criterio de fiabilidad ni de prudencia.

Imponer un criterio de seguridad, es sentar las bases para que queden fuera los criterios menos seguros, no legislados en la ley, pero si utilizados en una transacción internacional por quien suele utilizarlos, como es el caso de los e-mails firmados electrónicamente, que pueden variar su validez en las distintas legislaciones estatales, estableciendo que los riesgos normales de fiabilidad puedan invalidar la firma electrónica, aunque su fiabilidad sea demostrable y, al contrario, que no sea válida la firma electrónica reconocida, porque los requisitos técnicos utilizados no sean permitidos en otro país[613].

Lo que está claro es que la función de una firma es vincular a una persona, física o jurídica, con un documento y que el tipo de firma puede establecer el efecto jurídico de esta unión[614]. Uno no puede saber este vínculo sin conocer el contexto, lo que nos lleva a pensar que el contexto debe ser idóneo para usar una determinada firma; para que,

[611] KELMAN, A.; CHISSICK, M.: *Electronic commerce: law and practice*, Londres, 2002, 94 y ss.
[612] MANSON, S.: *Electronic signature in Law*, Cambridge, 2011, pág.105 y ss.
[613] GREGORY, J.D.: "Must e-signature be reliable?" *Digital evidence and electronic signature law review*, octubre, 2013, núm. 10, págs.67 – 70.
[614] BRAZEL, L: *Electronic Signatures, Law and Regulation,* Oxford, 2005, págs. 45 y ss.

posteriormente, sea demostrada y no conlleve problemas añadidos. Esto puede ser fácil o ser difícil, todo dependerá de cómo se legisle.

Un hecho importante a tener en cuenta en la firma electrónica es la intencionalidad. Cuando estamos ante una negociación, la intencionalidad crea un documento electrónico que, con independencia de la firma que se utilice para validarlo, lo importante es la información que por cualquier medio, y a toda costa, quiere enviar a la parte que confía en el remitente[615] y, por tanto, el firmante de la transacción desea dar validez y solidez. La prudencia sería un elemento importante a seguir, con el fin de generar en la persona que recibe una seguridad, no en el uso de una técnica o de una tecnología determinada.

Fijémonos que, en todo estudio sobre la firma electrónica, siempre se parte de la comparativa de las firmas manuscrita y electrónica. Puestos a realizar comparaciones entre estas firmas, la respuesta a la pregunta, si alguien aceptaría un contrato firmado a pie de página con una "x", también puede hacerse, en referencia a un contrato electrónico firmado electrónicamente, poniendo a pie de página "Soy yo". Ante esto, nos encontramos que la prudencia nos lleva a valorar la buena fe, la fiabilidad y el riesgo, elementos esenciales en la emisión de cualquier tipo de firma electrónica[616].

Al hablar de prudencia lo hacemos teniendo en cuenta que, quien realiza la transacción es conocedor del medio que utiliza y, más aún, si tenemos en cuenta que, normalmente, como nos han comentado empresas consultadas: "quien realiza un negocio jurídico en línea tiene un asesoramiento técnico detrás". Al respecto, volvemos a hacer referencia a los métodos, que pueden ser tenidos en cuenta, referidos en la Guía para la incorporación de la Ley Modelo sobre Comercio Electrónico[617], con respecto al Artículo mencionado anteriormente, atendiendo a factores jurídicos, técnicos y comerciales: "1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de firma con

[615] KAH LENG, T.: "Have you signed your electronic contract?" *Computer Law and Security Review*, febrero, 2011, vol. 27, nº 1, págs. 75 – 82.
[616] DAVINSON, A.: "*The law of electronic commerce*, Cambridge, 2009, págs.93 y ss.
[617] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMCE* (2001), Nueva York, párr. 58.

arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente".

Sin embargo, siempre puede darse el caso en el que la parte que confía sabe de la persona que firma, pero trata de evitar el acuerdo, diciendo que la firma electrónica utilizada no era lo suficientemente fiable para que pueda realizarse la operación, actuando de mala fe. Ante esto, las legislaciones de los Estados deberían tener presente la Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales que en su Artículo 9,3-b) nos dice que: "cuando la Ley requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica: b) Si el método empleado: i) O bien es tan fiable como sea apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o ii) Se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas en el apartado a) supra".

Esta disposición fue adoptada, por la Comisión, tras escuchar expresiones de inquietud, en el sentido de que una firma electrónica solo podía satisfacer el requisito legal correspondiente, si el método de firma era suficientemente fiable a los efectos de la comunicación electrónica, atendidas todas las circunstancias del caso. Como eso solo lo podía determinar a *posteriori* un Tribunal u otro verificador de los hechos, las partes en una comunicación electrónica o en un contrato electrónico no podían saber con certeza, por adelantado, si la firma electrónica utilizada sería considerada

"suficientemente fiable" o si se le negaría validez jurídica por no haber cumplido éste requisito.

Esto daba pie a que, aun cuando no se discutiera la identidad del firmante o el hecho de firmar, aunque no surgiera una controversia en cuanto a la autenticidad de la firma electrónica, un Tribunal pudiera decidir, de todos modos, que la firma electrónica no era suficientemente fiable y, en consecuencia, invalidar el contrato en su totalidad. Eso conllevaba inseguridad, ya que se prestaba para que la parte en una operación, en que se exigiera una firma, tratara de soslayar sus obligaciones negando validez a su firma (o a la firma de otra parte), no sobre la base de que el supuesto firmante no hubiera firmado, o de que el documento que firmó hubiese sido modificado, sino únicamente sobre la base de que el método empleado para la firma no era suficientemente fiable en esas circunstancias. Se expresó firme apoyo en favor de mantener la "prueba de fiabilidad" enunciada en el apartado b) del párrafo 3[618].

Al reconocerse lo anterior, la propia CNUDMI[619] indicó que el requisito de identidad, enunciado en el apartado a) del párrafo 3 del proyecto de Artículo 9, podía ser insuficiente para garantizar la interpretación correcta del principio de equivalencia funcional de las firmas electrónicas, porque la prueba de fiabilidad enunciada en ese apartado, al tiempo que establecía los requisitos mínimos para la validez de la firma, también recordaría a los Tribunales la necesidad de tener en cuenta otros factores que no fueran de carácter tecnológico, al tratar de determinar la validez de la firma; por ejemplo, el fin con que fue generada o transmitida la comunicación electrónica, o un acuerdo pertinente concertado por las partes. Sin el apartado b), los Tribunales de algunos Estados podían sentirse inclinados a considerar, que solo los métodos de firma que emplearan dispositivos de seguridad de alto nivel, eran adecuados para identificar a las partes, aunque éstas hubiesen convenido utilizar métodos de firma más sencillos.

No le falta razón a la CNUDMI, pues el desafío al que se enfrenta la firma electrónica, para su reconocimiento transfronterizo, es al establecimiento de un enfoque uniforme y confiable para la emisión y gestión de credenciales de identidad electrónica

[618] CNUDMI/UNCITRAL: *Anuario volumen XXXVI: 2005*, Nueva York, 2010, párr. 65 a 68.
[619] CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 147 y ss.

en las firmas electrónicas[620]. Sin un estándar de aseguramiento de identidad electrónica uniforme, que esté alineado con las diversas leyes de firmas nacionales, todas partes presentes en la transacción se enfrentan a la necesidad de poseer varios tipos de credenciales electrónicos. Al mismo tiempo, cada parte que confía debe saber que credencial electrónico y que firma electrónica tiene, en un país, la misma validez jurídica y es confiable como credencial electrónico en cualquier otro país[621]. Sin un estándar de aseguramiento de una e-identidad uniforme, que esté alineado con las diversas leyes de firmas nacionales en el control de acceso de la industria emergente y los requisitos de mensajería seguros, los notarios de todo el mundo se enfrentan a la necesidad de poseer varios tipos credenciales electrónicos.

Por ello, las leyes deberían tener como objetivo establecer un nivel de aseguramiento universal, confiable para la unión de identidades, con el fin de establecer credenciales aceptables en cualquier país. Esto es de vital importancia, si se tiene en cuenta que la integridad del contenido del documento electrónico y la firma, se basa en la capacidad de identificar al firmante o al remitente del documento de manera real y confiable.

De esto se ha hecho eco la Unión Europea, que con el Reglamento Nº 910/2014 del Parlamento y el Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[622], y por el que se deroga la Directiva 1999/93/CE, trata de armonizar la identificación electrónica en los Estados miembros. Aunque es cierto que no realiza un desarrollo de identificación electrónica de hecho; pues, reconoce que la regulación de la prueba de identidad es competencia nacional y respeta los principios de subsidiaridad y proporcionalidad.

[620] Obsérvese, esto es lo que se pretende realizar, en la Unión Europea, con el Reglamento Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
[621] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", *e*n *Comercio electrónico: estructura operativa y jurídica* (dirs. R.A. Etcheverry y R. Illescas Ortiz), Buenos Aires, 2010, págs. 169 – 259.
[622] Bruselas, 4/6/2012 COM (2012) 238 final (2012/0146 (COD)).

5.2.3. Elementos implicados en la emisión de las firmas electrónicas simples

Íntimamente ligada a la validez y eficacia normativa de la firma electrónica simple, se encuentra la forma en que se emite. Como hemos dicho anteriormente, la prudencia nos lleva a valorar la buena fe, la fiabilidad y el riesgo, elementos esenciales en la emisión de cualquier tipo de firma electrónica.

5.2.3.1. Buena fe

La dificultad que podemos encontrarnos, en el contexto electrónico internacional, es que las partes se fíen de la oferta o de la transacción, que realizan y la acepten de buena fe. Internet permite dirigir información personalizada y detallada y la tecnología actual permite que los contratos se celebren casi instantáneamente o, al menos, crear la impresión de que se ha celebrado un contrato.

La buena fe, sabemos, no opera sólo en una dirección, sino que implica una carga de lealtad recíproca. Es consecuencia de un valor paradigmático del acuerdo, como posibilitador de aquellas relaciones humanas que se forman fuera del marco de lo afectivo y que no encuentran fundamento estricto en las relaciones de poder[623]. Así, la buena fe, como depósito conceptual de los valores comunitarios, impone consecuencias que van más allá del interés individual y hasta del interés de la otra parte contratante. La invocación de la buena fe es manifestación del postulado de la inalterabilidad del derecho preexistente, de las obligaciones privadas en la contratación electrónica, configurándose como un postulado de afirmación necesaria ante la complejidad del medio[624].

[623] MATTA, L. F.: "Contestación al discurso de instalación de la Profesora Olga Soler Bonnin", artículo correspondiente a *Real Academia de Jurisprudencia y Legislación*, Puerto Rico, 2013.
Disponible en: http://academiajurisprudenciapr.org/new/contestacion-al-discurso-de-la-profesora-olga-soler-bonnin/ (Última visita: 12/3/2014).
[624] ILLESCAS ORTÍZ, R: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 58.

5.2.3.2. Fiabilidad

La aceptación de la firma puede realizarse a través de la aceptación de la oferta o en la comunicación previa que se realiza. La aceptación, en general, se puede hacer de cualquier forma, siempre que sea razonable a las circunstancias. La fiabilidad del método determinará la confianza. Fijémonos que la mayoría de los contratos on-line se forman mediante un simple "clic", mediante el uso de una contraseña y usuario, a través de un correo electrónico, etc.[625]

La exigibilidad de la firma electrónica sólo se establece una vez que ambas partes hayan dado su consentimiento para que se cumpla con los requisitos de la firma manuscrita, bajo la Ley de firma electrónica de la jurisdicción donde se aplique o se está utilizando, como una cuestión de prueba de la conducta; es decir, a través de la firma se está asumiendo una forma de involucrar a la persona que se identifica con la marca en un documento. En este punto, entra en juego el requisito de fiabilidad: si la forma o el método utilizado es suficientemente fiable para identificar al firmante e indicar que este firmante aprueba la información, que se encuentra en el documento[626].

Todo va a depender del sentido que le demos a la palabra identificar[627]: por un lado, si entendemos que la prueba de identidad va a implicar un proceso de adecuación de la prueba, que se presenta con los hechos conocidos con anterioridad acerca de esa persona; o sea, la fiabilidad de todo el proceso va a depender del alcance, de los hechos conocidos con anterioridad y de la precisión de la coincidencia entre los datos que se presenten en el documento electrónico; por otro, si vamos a entender identificar como vincular al firmante con el mensaje, la fiabilidad dependerá de la facilidad con la que alguien podría hacerse pasar por el firmante o la probabilidad de que alguien pueda hacerlo.

---

[625] HEDLEY, S.: *The Law of electronic commerce and the internet in the UK and Ireland*, Londres, 2006, págs. 244 y ss.
[626] GREGORY, J.D.: "Must e-signature be reliable?" *Digital evidence and electronic signature law review*, octubre, 2013, núm. 10, págs.67 – 70.
[627] SMEDINGHOFF, T. J.: "Solving the legal challenges of trustworthy online identity", *Computer Law and Security Review*, octubre, 2012, vol. 28, núm. 5, págs. 532- 541.

Ahora bien, preguntémonos si un mensaje de correo electrónico firmado con un nombre, o cualquier medio que nos permita utilizar una firma electrónica simple, garantiza una deuda, un contrato, una transacción, etc. En primer lugar, debemos ver el reconocimiento de los documentos electrónicos, incluyendo correos electrónicos, para ver con posterioridad el reconocimiento de la firma, para observar qué requisitos se exigen en los distintos ordenamientos jurídicos.

Esta cuestión, en los países de la *common law*, se remonta a sus antecedentes ingleses, cuyo origen concreto se sitúa en la Ley de 1677 del *Statute of Frauds*[628]. Es importante tener en cuenta que esta Ley de 1677 fue promulgada, como dice en su preámbulo, "para la prevención de muchas prácticas fraudulentas". De hecho, en el caso *Steadman v Steadman*[629], se dice que "antes, algunas transacciones se llevaban a cabo vía oral, de tal forma que los intereses que estaban en juego podían verse afectados negativamente. El remedio era exigir una mayor formalidad en el registro de dicha transacción. De esta forma, se trataba de proteger a las personas y a sus bienes contra el fraude, legislando qué tipos de contratos no podían hacerse cumplir, a menos que hubiera una prueba escrita de su existencia".

Conforme al derecho anglosajón sobre las pruebas en lo civil, se considera que una información consignada en papel o un documento, puede ser auténtico si existen pruebas de que el documento o la información consignada en el papel es lo que afirma el proponente. La pertinencia de un documento, como elemento de prueba, se establece al vincularlo a una persona, lugar o cosa; proceso que en algunos foros de derecho anglosajón se denomina autenticación. Firmar un documento es un medio habitual de autenticación, y, según el contexto, las expresiones "firmar" y "autenticar" pueden utilizarse como sinónimos[630].

La definición de firma se puede resumir en el caso *Goodman v J Eban Ltd*.[631], caso dado en el marco del derecho inglés, que viene a decir que, cuando la Ley requiere que cualquier documento, en particular, este firmado por una persona; a primera vista, el

[628] Disponible en: http://www.legislation.gov.uk/aep/Cha2/29/3/contents (última visita: 13/3/2014)
[629] REINO UNIDO: Steadman v Steadman [1976] AC 536 (" *Steadman* ").
[630] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 2.
[631] REINO UNIDO: Goodman v J Eban ltd (J) Ltd. [1954] 1 All ER 763.

requisito exigido por la Ley se cumple si, la persona misma pone en el documento algún "grabado" que represente su firma por medio de un sello de goma; es decir, el requisito esencial de la firma es la colocación de alguna manera, ya sea por escrito, con una pluma o un lápiz o, por el contrario, por impresión en el documento, el nombre de uno o la firma representada por un signo; a fin de, personalmente, autenticar el documento. Asimismo, en el caso *Re a Debtor*[632], el Tribunal consideró que un documento firmado y enviado por fax puede dar como firmado legalmente. En opinión del Tribunal, resulta difícil ver por qué algunos métodos de realizar una marca sobre el papel sean más válidos que otros, de esta forma sugirió que si la firma se digitalizó y posteriormente se añade al fax, el documento debe considerarse como firmado.

En virtud de estas amplias interpretaciones de la firma, puede considerarse que, simplemente, escribiendo el nombre de la persona al final de un correo electrónico, puede que sea suficiente. Además, en el archivo adjuntado al e-mail puede añadirse una firma; por ejemplo, en un documento con membrete y, por lo tanto, también podría considerarse una firma[633]. Lo que podemos apreciar en el en el caso *Mehta v J Pereira Fernandes SA*[634], en el cual, haciendo referencia a la Ley de comunicaciones electrónicas de Reino Unido, y al *Statute of Frauds*, el Tribunal sostiene que sin un nombre escrito al final del mensaje, no hay ninguna firma efectiva, pronunciamiento que, según el Tribunal, es coherente con la jurisprudencia existente.

De esta forma, al igual que una "x" o alguna otra marca puede considerarse como una firma, casos como los que se han dado en Australia confirman este hecho, por ejemplo, en el caso *R. contra Moore: ex part Myers*[635], el Tribunal permitió que un nombre impreso fuera suficiente para considerar la firma como vinculante, declarando que una "firma es sólo una marca" y puede "ser impresa sobre el documento con un sello grabado con un facsímil de la firma habitual de la persona que firma". El término firma electrónica no significa una firma digitalizada ni una firma digital. Una firma digital es un tipo específico de firma electrónica segura, a veces referido como un certificado digital.

[632] ESTADOS UNIDOS: Re a Debtor (Nº. 2021 de 1995) [1996] 2 All E.R. 345 a 351.
[633] CHISSICK, M.; KELMAN, A.: *Electronic commerce: law and practice*, Londres, 2002, pág. 97 y ss.
[634] REINO UNIDO: Mehta v J Pereira Fernandes SA" [2006] EWHC 813 (Ch).
[635] AUTRALIA: R. v. Moore: ex part Myers (1884) 10 V.L.R. 322 at 324 (Reino Unido, Victorian Law Reports).

En el caso *R v Frolchenko*[636], la Corte de Apelaciones de Queensland declaró que dicho documento electrónico puede ser autenticado, examinando otros factores, tales como si el nombre aparece en escritura tipo o al final del documento. En el caso *McGuren v Simpson*[637], el Tribunal dijo que la palabra "firma" se ha interpretado de manera muy informal. De esta manera, una hoja impresa puede ser suficiente si contiene el nombre de la parte demandada.

En EE.UU, en el *caso* Doherty v. Registry *of Motor Vehicles*[638] el Tribunal consideró válido un informe de la policía hecho por medio de correo electrónico y firmado al final con el nombre del policía, al establecer que, "además, podría haberse hecho por cualquier otro medio electrónico", de la misma manera que el oficial informante, si no fuera real se somete a posibles cargos de perjurio. Igual sentido ha adoptado el Tribunal de Apelación de Estados Unidos, que en el caso *Cloud Corp. v. Hasbro Inc.*[639], que llegó a la conclusión de que "el nombre del remitente en un correo electrónico satisface la firma exigida en la ley contra el fraude".

Visto lo anterior, parece claro que, en el derecho anglosajón, existe un punto en común muy arraigado; pues, un simple nombre al final de un correo puede considerarse como apoyo suficiente para certificar la persona que lo envía[640]. Al mismo tiempo, es necesario decir que el efecto de las comunicaciones electrónicas sobre las cuestiones jurídicas sigue evolucionando.

Observemos que, el Tribunal de Apelación de Singapur, en el caso *Joseph Mathew y Otro v Singh Chiranjeev*[641], llega a esta conclusión, pareciéndole de justicia y de sentido común, que los negocios se están realizando, hoy día, por medios electrónicos, en lugar de cartas escritas en papel y, en el futuro, la proporción de negocios que se van a realizar por vía electrónica no hará sino aumentar. De esta forma, el hombre de la calle, que no sólo lleva a cabo negocios a través del ordenador, fomenta

[636] AUSTRALIA: R v Frolchenko (1998) QCA 043 (20 de marzo de 1998).
[637] AUTRALIA: McGuren v Simpson" [2004] NSWSC 35 (18 de febrero 2004).
[638] ESTADOS UNIDOS: Doherty v. Registry of Motor Vehicles No. 97 CV 0050 (1997).
[639] AUTRALIA: Cloud Corp. v. Hasbro Inc.", 314 F.3d 289 (2002).
[640] DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009, pág.108.
[641] SINGAPUR: Joseph Mathew y Otro v Singh Chiranjeev (y Otro [2009] ASGC 51, de fecha de 29 de octubre de 2009).

el uso de tecnología en todos los ámbitos de la vida y es fácil darse cuenta de que cada vez hay más y más conocimientos tecnológicos. Por ello, sorprende al Tribunal que las leyes no reconozcan un contrato firmado electrónicamente a pesar de que todos los términos del contrato se hayan acordado y desarrollado en formato electrónico y, además, las partes son perfectamente identificables. Si las partes que negocian electrónicamente no desean estar unidos hasta que se firme un documento formal, pueden recurrir a las cláusulas del contrato que se pueden agregar fácilmente a su correspondiente correo electrónico.

El Tribunal resuelve, dando un paso más en los casos mencionados anteriormente, diciendo que no anexar un nombre en la parte inferior de cualquiera de los mensajes de correo electrónico no tiene importancia. Todos los mensajes de correo electrónico incluyen, una fecha y un envío a la otra parte y tienen, cerca del inicio de la misma, una lectura de la línea superior que "dice " De: "Tan Tian Tye". Es cierto que la persona que envió el mensaje confirmó que los había enviado, de igual manera no había duda de que en el momento en que los envió, tenía la intención de enviarlos. A pesar de eso no consideró necesario identificarse como remitente, añadiendo su nombre al final de cualquiera de los mensajes de correo electrónico. De esta forma, se infiere que la omisión de escribir su nombre se debe a su conocimiento de que su nombre apareció en la cabecera de cada mensaje, junto a su dirección de correo electrónico, tan claramente que no había ninguna duda de que estaba destinado a ser identificado como el remitente del mensaje de este tipo".

Con todo lo anterior, parece que se empiezan a fijar criterios ampliados para la fiabilidad, así como las normas de conducta, diseñados para facilitar el reconocimiento y el uso de la firma. Los Tribunales, en los países anglosajones estudiados, parecen haber adoptado posturas indulgentes a la hora de aceptar las firmas electrónicas, reduciendo la admisibilidad a una demostración de la fiabilidad.

5.2.3.3. El riesgo

Las posturas indulgentes, a la hora de aceptar la demostración de fiabilidad de la firma electrónica simple, parecen estar siendo analizada por los Tribunales, con el fin de

establecer excepciones a la regla general, que se ha venido desarrollando hasta ahora. Veamos, por ejemplo, el caso *In Re Vee Vinhnee*[642], en el que se negó a admitir registros de transacciones de tarjetas de crédito electrónicas debido a una autenticación insuficiente.

Parece que se está tratando de desarrollar judicialmente un proceso de firma electrónica efectiva, a través del cual se tengan en cuenta los aspectos jurídicos y prácticos más allá de las Leyes de firma electrónica[643]. En este proceso, se debe tener presente una serie de riesgos, a partir de los cuales se permita ver qué medidas son necesarias para mitigar el riesgo de manera aceptable, para que el proceso de firma electrónica pueda darse con éxito.

En otras palabras, se trata de establecer un proceso de firma electrónica confiable; por ejemplo, para la compra de un libro barato, que, en un principio, no es el mismo o no tiene por qué ser tan seguro como para comprar; por ejemplo, un artículo costoso (una casa, un collar o unas gafas de sol de gran valor, maquinaria pesada, etc.) que puede conllevar a la autorización de una determinada información mucho más sensible, aunque partamos de la base de que toda información es sensible.

En este sentido, en el caso *Lorraine v. Markel American Ins. Co*.[644], se establece un importante análisis detallado de los fundamentos probatorios, a tener en cuenta a cerca de la admisibilidad de la prueba electrónica. El Tribunal sostuvo que cada vez que los documentos electrónicos son ofrecidos como prueba, se debe considerar lo siguiente:

a) Autenticidad de la información dada: lo que se traduce en el riesgo de que uno de los firmantes de hecho, no sea la persona que dice ser. Un usuario puede autenticar la identidad de cada firmante de varias maneras. La identidad de cada persona que firme debe ser verificada. Estas medidas de

[642] ESTADOS UNIDOS: In Re Vee Vinhnee, 336 B.R. 437 (9th Cir. BAP (Cal.) 2005).
[643] CURRY, S.: *"*Washington's electronic signature Act: an anachronism in the new millennium", *Washington Law Review*, junio, 2013, vol. 88, núm. 2, págs. 2- 16.
[644] ESTADOS UNIDOS: Lorraine v. Markel American Ins. Co. 241 F.R.D. 534, 538 (d. Md. 2007).

verificación pueden incluir la confirmación de la identidad de dicha persona, a partir de una fuente de confianza.

b) Que de los documentos presentados para hacer cumplir la transacción pueda deducirse que son verdaderos; o sea, que se pueda deducir a través del proceso de firma electrónica, que el documento generado, se asocia de manera lógica con el documento, que el propio firmante firmó electrónicamente. Surge así, el riesgo de que el firmante repudie el documento adjunto o lógicamente asociado con su firma. Con ello, puede que se reduzca la posibilidad de que el documento sea admisible y, de ser admitida como prueba, se pruebe que el firmante no estaba de acuerdo en obligarse por todos sus términos y condiciones.

c) Que las pruebas que se presenten constituyan un "original"; es decir, que los documentos presentados para hacer cumplir la transacción son verdaderos, exactos y completos de copias impresas de cada documento firmado por cada firmante, que refleja con exactitud lo que el firmante presentó. Todo siempre en el marco de cada firmante, utilizando el proceso de firma electrónica;

d) Que el valor probatorio, de las pruebas electrónicas, debe superar sustancialmente cualquier peligro de prejuicio injusto o cualquier otro factor identificado.

De esta forma, se trata de atender al riesgo que puede conllevar una operación, en el sentido de que es necesario, porque así lo hemos constatado en la preocupación de empresarios y consumidores, para establecer un proceso de firma lo suficientemente ágil y poco arriesgado, como para poder permitir a las partes tener una visión subjetiva de los riesgos que tienen en juego[645]; o sea, de las distintas posibilidades que tienen de actuar para, finalmente, determinar cuáles son los medios óptimos para mitigar cualquier miedo o riesgo que pueda surgir, hablando siempre desde un punto de vista internacional.

[645] SCHAPPER, P.R.; RIVOLTA, M.; VEIGA, J.: "Risk and law in authentication", *Digital evidence and electronic signature law review*, octubre, 2006, núm. 6, págs. 12- 18.

Por este motivo, es probable que tengamos que determinar si una firma electrónica es válida o no, observando[646]: 1) el tipo de acuerdo que se firmó, 2) el tipo de firma electrónica que se está utilizando, y 3) la forma en que cada parte consiente el uso de la firma electrónica.

Con lo anterior, surgen cuestiones importantes que nos podrían valer para todo tipo de firma electrónica[647] (sea simple o digital):

1) Si las transacciones ejecutadas, utilizando el proceso de firma electrónica propuesto en el contrato, están en consonancia con las leyes aplicables que rigen el uso de la firma y la entrega de los documentos electrónicos relacionados.

2) Si los documentos electrónicos presentados, firmados, archivados y recuperados mediante el proceso de firma electrónica propuesto en el contrato son admisibles ante un tribunal.

3) Si los términos y condiciones en los documentos electrónicos firmados, utilizando los materiales de proceso de firma electrónica, serán ejecutables contra cada parte firmante.

El marco para responder a estas cuestiones se sitúa dentro del propio proceso de firma electrónica, que se desarrolla en el entorno de cada transacción, que podemos situar dentro del proceso de contratación. Esto se traduce en como poder conseguir que sea admisible este proceso de contratación; es decir, como hacer cumplir los términos y condiciones firmados electrónicamente por las partes. Todo esto, lógicamente, nos lleva al proceso de la prueba.

En la investigación de esta cuestión hemos tratado de buscar una solución amplia que nos lleve a resolver el problema específico que se nos presenta o que, al menos, nos

[646] NORTON, W. K.: "Enforcing 'simple' electronic signatures in an international context", *Digital evidence and electronic signature law review,* octubre, 2012, núm.9, págs.74 – 78.
[647] SCHAPPER, P.R.; RIVOLTA, M.; VEIGA, J.: "Risk and law in authentication", *Digital evidence and electronic signature law review,* octubre, 2006, núm. 6, págs.12- 18).

permita dar un punto de partida sobre la admisibilidad de la firma electrónica simple, como prueba válida en cualquier transacción.

En este punto, nos podemos preguntar, si pueden ser presentados como pruebas[648] y considerados como válidos en juicio; por ejemplo, e-mails o documentos electrónicos firmados de la forma más simple[649].

Si tengo una carta en formato papel lo primero que nos preguntamos es si ésta es una falsificación. Tras la prueba realizada por un perito, si es una falsificación, la firma no plantea problemas; pues, no tenemos por qué tenerla en cuenta. Si es verdadera es cuando nos planteamos si la firma es una falsificación. De igual manera, debe ser con el e-mail: si un amigo, conocido o cualquier persona que realiza transacciones comerciales, afirma que la dirección de correo es falsa, el estatus de la firma electrónica que acompaña al e-mail resulta irrelevante, pero lo cierto es que nadie puede falsificar un e-mail y luego escribir cualquier nombre como firma electrónica[650].

Observemos que la verificación del e-mail se produce antes que la verificación de la firma. El e-mail, en toda relación comercial, se repite entre las partes y genera una confianza, sólo lo conocen las partes y si a esto se le añade un nombre, un apellido y, además, el puesto que ocupa en la empresa o, en su defecto, algún rasgo que ayude a la identificación, más aún. De esta manera, se puede decir que solo las partes suelen autenticar el contenido del mensaje electrónico.

Tengamos en cuenta que en la mayoría de los casos, en la práctica, en los que se contrata a través de una web, se requiere un registro electrónico, también cuando se inicia algún procedimiento con la administración e, incluso, cuando se hace inscribe para el uso posterior de una cuenta de correo electrónico (véase por, por ejemplo, como PayPal te hace rellenar un formulario y vincularte con un cuenta de correo electrónico). Casi siempre se rellena un formulario en el que uno se identifica y se hace accesible a través de una dirección de correo electrónico que se indica previamente. Con esa dirección acepto la recepción de documentos de pago (por ejemplo, facturas o algún tipo

[648] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, págs. 259 y ss.
[649] ESLER, B. W.: "Lorraine v Markel: unnecessarily raising the standard for admissibility of electronic evidence", *Digital evidence and electronic signature law review*, octubre, 2007, núm. 4, págs. 80 – 82.
[650] ESTADOS UNIDOS: Lorraine v. Markel American Ins. Co. 241 F.R.D. 534, 538 (d. Md. 2007).

de comprobante de que la compra se ha efectuado), confirmación de pedidos, confirmación de pagos, se permite hacer un seguimiento de los productos que se han adquirido, etc. Ante esto, resulta difícil no quedar obligado por las circunstancias.

Posteriormente, el documento firmado y enviado, incluso cuando es en formato digital, a veces, requiere la comparación con un estándar digno de confianza; o sea, con el original[651].

La referencia al original es, simplemente, el objeto con el que se acuerda con la otra parte confiar y autenticar en comparación con otros objetos, que bien pueden ser objetos que me ha suministrado o bien e-mails que nos hemos enviado.

Solo de esta forma, llegamos a una referencia propia que nos da confianza. Esta referencia es la que nos lleva a pensar en que hay una identidad que se asocia al mensaje y esa identidad lo está declarando como válido. Porque se está reconociendo como válida la identidad de la otra persona que protege y defiende la inmutabilidad del documento objeto de confianza.

Ante la situación que se plantea y que coincide con la práctica real empresarial, no se hace necesaria tecnología alguna, basta con una promesa de que la información no va a cambiar en el tiempo. Así pues, se atiende a la importancia de la transacción, de manera que cuando una empresa firma o hace una declaración electrónica de carácter contractual es porque la parte contratante piensa que le ha demostrado que es quien dice que ser.

Por consiguiente, la persona confía en la firma, aunque surja el riesgo[652] de que no es quien dice ser y debe actuar en consecuencia: evaluando el riesgo y protegerse de la misma. Por ello, en el balance del riesgo está la confiabilidad, que nos llevará a una firma más fiable y/o más segura.

[651] HATFIELD, P.; CASAMENTO, G.: "The essential elements of an effective electronic signature process", *Digital evidence and electronic signature law review*, octubre, 2009, núm. 6, págs. 83 – 97.
[652] SCHAPPER, P.R.; RIVOLTA, M.; VEIGA, J.: "Risk and law in authentication", *Digital evidence and electronic signature law review*, octubre, 2006, núm. 6, págs.12- 18).

En este contexto, se demuestra la importancia de la firma electrónica, como proceso individualizado, pero no en el concepto que a menudo se detalla, con un trato tecnológico claramente preferencial, que si bien pueden presentarse como referencia válida no puede darse como la única presunción válida.

5.2.4. Requisitos añadidos para la validez de las firmas electrónicas simples

Resulta claro que si la firma manuscrita se remite a un documento en soporte escrito, la firma electrónica se remite a un documento en soporte electrónico[653]. La cuestión que se nos presenta está en: si en virtud de la función que va a desempeñar la firma electrónica vale cualquier forma o, por el contrario, necesita una determinada forma de firma electrónica para cumplir una determinada función.

Algunas Leyes, sobre firma electrónica, reflejan una clara distinción entre la noción de intención y la idea de seguridad[654]. Así, al aplicar la firma electrónica suele establecerse como presunción previa, que los acuerdos requieren el equivalente a la firma manuscrita, presunción de validez que se le suele dar solo a una determinada firma electrónica.

La primera cuestión la hemos tratado anteriormente, al desarrollar la interpretación flexible, que han tendido a interpretar los requisitos de firma los Tribunales en los países anglosajones, donde con mayor frecuencia, al interpretar las normativa contra el fraude, se han mostrado abiertos al reconocimiento legal de la firma electrónica y han permitido, que se utilice en situaciones no previstas, expresamente, en la norma, autorizando su empleo o su expedición, a través de mandamientos judiciales[655]. Y lo que es más importante, en el contexto contractual, los Tribunales, también, han evaluado la idoneidad de la autenticación conforme al trato establecido entre las partes, en lugar de aplicar una norma estricta en todas las situaciones.

[653] CRUZ RIVERO, D.: *Eficacia probatoria de la firma electrónica*, Madrid, 2006, págs. 259 y ss.
[654] MANSON, S.: *Electronic signature in Law*, Cambridge, 2011, pág.115 y ss.
[655] FORDER, J.: "The inadequate legislative response to e-signatures", *Computer Law and Security Review*, Julio, 2010, Vol. 26, núm. 4, págs. 418 – 426.

A tenor de lo comentado, tanto en Estados Unidos como en Australia y en Reino Unido, no parece haber precedentes de denegación por un Tribunal de los mensajes de correo electrónico y con nombres mecanografiados en ellos, que no cumplan los requisitos relativos a la forma escrita y a la firma prevista en la legislación[656]. Si se deniega; por ejemplo, como en el caso *Pretty Pictures Sarl v Quixote Films Ltd*.[657], que refleja negociaciones en curso y acuerdos no definitivos, porque durante esas negociaciones, una de las partes, había previsto que se celebrara un contrato vinculante, únicamente, después de que se firmara un "memorando de negociación".

Cierto es que los Tribunales británicos parecen interpretar los requisitos de forma previsto en la Ley del Fraude de manera más estricta, aunque se inclinan, por lo general, a admitir la utilización de cualquier método de firma o autenticación electrónica, incluso, sin que lo autorice una legislación determinada, siempre y cuando que el método en cuestión cumpla la misma función que la firma manuscrita.

La segunda cuestión, planteada al inicio de este apartado, se suele dar en los países europeos, donde se aplica un enfoque más restrictivo, respetando mucho la forma. Posiblemente, porque en muchos de ellos el concepto de "documento" supone, habitualmente, algún tipo de autenticación, como es en el caso de España, lo que dificulta disociarlo de la "firma"[658]. Cuando los requisitos legales de forma se miran con detalle, por lo general, surgen diferencias de criterios. No obstante, en común con todas las Leyes, sobre firma electrónica, influenciadas por la Directiva 1999/93/CE y la Directiva 2000/31/CE, observamos similitudes en las funcionales que llevan, posteriormente, a dar determinados requisitos de forma:

a) Una función probatoria: la exigencia de un requisito de forma es, a menudo, un requisito presuntivo probatorio satisfactorio, antes de realizar una transacción.

[656] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 108.
[657] AUSTRALIA: Pretty Pictures Sarl v Quixote Films Ltd" 16 [2003] All ER (D) 303 (Jan).
[658] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 109.

b) Una función de advertencia: al exigir una formalidad, que requiere algún esfuerzo. La ley disuade a la gente de entrar en este tipo de operaciones de forma impulsiva.

c) Una función de canalización: para facilitar la regulación jurídica de determinados tipos de operaciones.

Así, la Directiva 2000/31/CE[659] nos dice que todo Estado miembro debe ajustar su legislación en cuanto a los requisitos y, especialmente, los requisitos formales, que puedan entorpecer la celebración de contratos por vía electrónica. El efecto jurídico de la firma electrónica era objeto de la Directiva 1999/93/CE[660] y, ahora, del Reglamento 910/2014, que no pretende armonizar las legislaciones nacionales sobre contratos, en particular, por lo que respecta al perfeccionamiento y eficacia de los mismos, ni tampoco otras formalidades de naturaleza no contractual relativas a la firma[661]. Por dicho motivo, las disposiciones sobre los efectos legales, de la firma electrónica, deberán entenderse sin perjuicio de los requisitos de forma establecidos por las legislaciones nacionales en materia de celebración de contratos, ni para las normas que determinan el lugar en que se considera celebrado un contrato.

[659] Considerando 34 de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) , nos dice que: "Todos los Estado miembro debe ajustar su legislación en cuanto a los requisitos -y, especialmente, los requisitos formales- que puedan entorpecer la celebración de contratos por vía electrónica. Se debe examinar de forma sistemática qué legislaciones necesitan proceder a dicho ajuste y este examen debe versar sobre todas las fases y actos necesarios para realizar el proceso contractual, incluyendo el registro del contrato. El resultado de dicho ajuste debería hacer posibles la celebración de contratos por vía electrónica. El efecto jurídico de la firma electrónica es objeto de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica. El acuse de recibo expedido por un prestador de servicios puede consistir en suministrar en línea un servicio pagado".

[660] Artículo 1 de la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, nos dice que: "firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior. La presente Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos".

[661] El Reglamento en su Artículo 1,3 nos dice que: "El presente Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma".

El criterio legislativo adoptado, respecto de la firma electrónica y su autenticación, ha influido en la actitud de los Tribunales. Las Leyes sobre firma electrónica, sin una norma general relativa a la autoría, han hecho que se preste atención sólo a la forma en que se puede desarrollar la función de los métodos de autenticación, relativa a la identidad, lo que genera desconfianza respecto de los métodos de autenticación. Aquí el Reglamento 910/2014 si establece una novedad, en cuanto a que fija las tres funciones de la firma electrónica, que hemos destacado en los capítulos anteriores: presta atención a la identificación (Artículo 3,1), a la autenticación (Artículo3,5) y a la firma electrónica (3,10), entendiendo esta última, como el método de autenticación.

Observemos que, en el caso *Mehta contra J. Pereira Fernandes S.A*[662], el Tribunal nos dice que la opinión, que la Comisión en la Directiva 2003/31/CE, refleja no querer requerir cambios respecto a las Leyes por las que se exija una firma, porque el cumplimiento de este requisito se puede demostrar funcionalmente, determinando si el comportamiento del posible firmante refleja intención de autenticar. Con ello, si una parte o su agente envían un correo electrónico y mecanografían su nombre en el texto del mensaje, dentro correo electrónico, conforme a lo exigido o permitido por la jurisprudencia, lo que, a juicio del Tribunal, constituiría una firma.

En España, el Tribunal Supremo, en Sentencia de 15 de junio de 2011, nos dice que para que "un documento privado no sea idóneo para constituir un medio de prueba es preciso que sea inauténtico; es decir, no provenga de su autor, de modo que no haya coincidencia entre el autor aparente y el autor real. Cuando un documento privado sea impugnado por la parte contraria a quien lo presentó, que lo estima perjudicial a sus intereses, a la parte que lo aportó al proceso, le incumbe la carga de probar la autenticidad, lo que no obsta a que la otra parte pueda, también, intentar acreditar la inautenticidad. Si se demuestra la falta de autenticidad, el documento carece de eficacia probatoria y si se acredita que es auténtico es plenamente idóneo para probar *per se*. Cuando no se pudiere deducir la autenticidad o no se hubiere propuesto prueba alguna, esto es, no consta que sea auténtico, pero tampoco inauténtico, el Tribunal lo valorará conforme a las reglas de la sana crítica. Para acreditar la autenticidad puede

[662] REINO UNIDO: Mehta v J Pereira Fernandes SA [2006] EWHC 813 (Ch).

utilizarse cualquier medio de prueba e incluso presunciones, en cuyo caso, la naturaleza de la prueba es la propia del medio empleado y no la del documento objeto de prueba".

En esta línea, la Sentencia de la Audiencia Provincial de Madrid, de 31 de mayo de 2013, en referencia a un correo electrónico firmado electrónicamente, establece que "no se pueden negar efectos jurídicos a una firma electrónica que no reúna los requisitos de la firma electrónica reconocida, en relación con los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica. Además, si se impugna la autenticidad, y aquí no se hizo en su momento, se estará a lo establecido en el apartado 2 del Artículo 326 LEC (Artículo 3,8 *in fine* LFE) con lo que volvemos al mismo punto de partida, porque en este caso quien presentó el documento podría pedir la pericial u otro medio de prueba".

En el mismo sentido, el Tribunal Supremo de Eslovenia, en Sentencia de 18 de junio de 2003, nos dice que los datos en forma electrónica no se le pueden negar validez por el simple hecho de estar en forma electrónica y que un correo electrónico es susceptible de ser de quien dice haberlo enviado, al declarar, explícitamente, que la validez o el valor de la prueba de una firma electrónica no puede rechazarse por el hecho de que no se base en un certificado reconocido o bien porque sea una firma electrónica menos segura[663].

Por el contrario, en Francia, en el caso *Société Chalets Boisson v MX* (Número 00-46467) de la *Cour de Cassation*, *Chambre Civile* 2, de fecha 30 de abril 2003[664]. En este asunto el 1 de abril de 1999 el Consejo de la Sociedad *Chalets Boisson* interpuso un recurso ante la *Cour d'Appel de Besançon*. La notificación de apelación se envió a la oficina del secretario de la Corte por e-mail, escribiendo su representante su nombre al final del correo. Esta apelación fue declarada nula, debido a que la firma electrónica, en su formato más simple y, por tanto, menos segura, se considera que no identifica al firmante. La *Cour d'Appel de Besançon* aceptó este argumento y declaró inadmisible el recurso de casación. El Tribunal de Casación avaló la decisión *Cour de Besançon* al establecer que, para ser válida "una apelación debe ser firmada por su autor y que la

[663] ESLOVENIA: Sentencia de la Corte Suprema de la Republica de Eslovenia, caso I UP 505/2003, 18 de junio de 2003.
[664] FRANCIA: Sentencia de la Corte de Casación, juzgado de lo civil, caso "Société Chalets Boisson v MX" (Número 00-46467), de fecha 30 de abril 2003.

firma electrónica simple no es suficiente para identificar al autor; pues, cualquier persona puede escribir un nombre en la parte inferior de un e-mail y no es seguro que la persona cuyo nombre se escribe al final del e-mail era la persona que lo envió".

La Corte adoptó una posición sistemática de desconfianza con respecto a la firma electrónica. Confirma que es el papel, y sólo el papel, lo que constituye la garantía legal de ser bueno. Sin embargo, Ley de 13 de marzo de 2000 y sus Decretos, de acuerdo con el Artículo 1386-3 del Código Civil: "la escritura en un soporte electrónico tiene el mismo valor probatorio que la escritura sobre un soporte de papel", pero no es menos cierto, que en virtud del Artículo 1316-2 del Código Civil: "el Juez decidirá en los conflictos de prueba, determinando por todos los medios, el título más probable sea cual sea el soporte". Este Artículo da a las partes libertad para acordar el uso de la firma electrónica que consideren. No obstante, si bien puede que no haya superioridad de un medio de prueba sobre otra, está claro que, para determinar el modo de prueba de qué es lo que más fiabilidad otorga, vendrá dado por el papel del Juez, que determinará la jerarquía del hecho, a la hora de establecer la prueba entre la firma electrónica y lo establecido en un papel.

A pesar de lo comentado, se observa una postura ligeramente más flexible, en que se acepta la presentación electrónica de recursos administrativos para cumplir un plazo legal, al menos si se confirman posteriormente por correo ordinario. Esta la observamos en la Resolución N º 88665 del el Consejo de Estado (de 8 de julio de 1988, *Bernhard Dietschi*) y Resolución N º 112949 (de 13 de marzo 1996, *Diraison*) que permiten la presentación de recursos en la forma de un télex[665].

En este último caso, el Consejo de Estado estableció, en su Resolución, que el recurso podría ser presentado por fax, puesto que éste contiene la exposición de los hechos, las conclusiones, los nombres y los domicilios de las partes. Además, con el fin de cumplir con todas las obligaciones de forma. Los solicitantes deben autenticar el recurso mediante la firma del documento que se envía. Ante esta forma de admitir esta la presentación de recursos, el Tribunal Administrativo de Nantes, en Sentencia de 7 de junio de 2001, validó el uso del correo electrónico para la presentación de éstos. Esta

[665] Disponibles ambas Resoluciones en: http://www.rajf.org/spip.php?article458 (última visita 13/3/2014).

validación se confirmó por el Consejo de Estado, en Resolución de 28 diciembre 2001, que dictaminó que el recurso fue enviado "por correo electrónico, recibido el 16 de marzo de 2001, y el solicitante, posteriormente, se confirmó como autor de éste recurso por la carta", por lo que dictaminó su admisión.

Recientemente, el Tribunal de Apelaciones de *Nancy*, en Sentencia 442/12, de 14 de febrero de 2013[666], hace referencia a la admisibilidad de un archivo de operaciones, como prueba de un contrato de préstamo firmado electrónicamente. El prestamista acordó con el prestatario un crédito renovable, en forma de línea de crédito. El valor del crédito fue objeto de tres modificaciones sucesivas por las cuales se aumentó la cuantía, las dos primeras mediante una firma manuscrita y la última, el 4 de septiembre de 2008, en forma electrónica. El crédito debía reembolsarse a plazos mensuales. En vista de que el prestatario había dejado de pagar las cuotas mensuales, desde el 5 de abril de 2009, el prestamista entabló una demanda ante el Tribunal, el 21 de enero de 2011, con el objeto de recuperar el crédito. El juez de primera instancia estimó que la firma electrónica de la última modificación carecía de validez y desestimó la demanda. Según el Juez, el archivo de operaciones que el prestamista aportó como prueba a las actuaciones era un "simple archivo impreso, sin garantía de autenticidad ni justificación del sistema de seguridad utilizado", de modo que esa firma electrónica no era suficientemente fiable para constituir la celebración de un contrato. En consecuencia, el Juez determinó que la última modificación "no había sido firmada" por el prestatario. De ahí que el Juez concluyera que el plazo de prescripción de dos años previsto en el Artículo L.311-52 del Código de Defensa del Consumidor regía a partir del 1 de marzo de 2006, fecha de la firma de la segunda modificación. El Juez determinó que al 21 de enero de 2011, fecha de presentación de la demanda, había expirado el plazo de dos años y, en consecuencia, desestimó la demanda. El prestamista presentó una apelación contra la decisión.

El Tribunal de Apelaciones revocó el fallo de primera instancia, reconociendo el mérito probatorio de la firma electrónica. Para llegar a esa conclusión, el Tribunal recordó ante todo que, en virtud del Artículo 1316-4 del Código Civil y del Decreto núm. 2001-272 de 30 de marzo de 2001, la firma electrónica "consiste en el uso de un

[666] CNUDMI/UNCITRAL: jurisprudencia relativa a los textos de la CNUDMI (CLOUT). A/CN.9/SER.C/ABSTRACTS/137. Publicado en origen: *La semaine juridique*, edición general, núm. 18, 29 de abril de 2013, pág. 867.

procedimiento fiable de identificación que garantice su relación con el acto al que se adjunta la firma. Se presume la fiabilidad de ese procedimiento, a menos que se pruebe lo contrario, cuando se crea la firma electrónica, se asegura la identidad del signatario y se garantiza la integridad del acto".

Sentido opuesto se muestra en Italia, donde el Tribunal de *Catanzaro*[667], en Sentencia de 23 de abril de 2012, dio la razón a un ciudadano, que iba a realizar una compra en línea de productos a una empresa de servicios informáticos y se opuso a que un sólo "clic" pudiera considerarse suficiente para realizar la operación.

El Tribunal hace referencia al Artículo 1341,2 del Código Civil italiano que establece expresamente que "en todo caso no tienen efecto las cláusulas que no han sido aceptadas expresamente por escrito, si éstas recogen condiciones que garanticen, a favor de la persona que lo ha preparado, limitaciones de responsabilidad". De esta forma, razona que "la aprobación expresa por escrito, expresada en el Artículo, depende de la manifestación de una voluntad, que sólo puede realizarse mediante firma electrónica reconocida".

La importancia de la decisión adoptada por el Tribunal de Justicia está en que "la aprobación específica por escrito de esta cláusula abusiva, que figura en el formulario de contratación on-line, debe requerir el uso de la firma electrónica digital, de lo contrario esto llevará consigo la ineficacia de la misma". De esta forma, se está diciendo que los contratos on-line, que contengan cláusulas individuales, deberán ser aprobadas por los usuarios mediante firma digital. Pues, la firma electrónica simple, puede que "identifique en algún caso, pero no avala".

En Alemania la especificación de una dirección de correo electrónico, o el nombre del remitente, a pie de página del correo electrónico, junto con la contraseña, no es un indicio suficiente de que ha habido una cierta persona que ha participado en una subasta en Internet. La expresión de una la dirección de correo electrónico, por lo tanto, no se trata de una prueba de la existencia de una aceptación de los votos en la oferta pública

[667] Disponible en: http://www.leggioggi.it/wp-content/uploads/2012/06/ordinanza-catanzaro_ebay.pdf (última visita 13/3/2013).

de subasta (Sentencia de *AG Bonn Urteil* de 25/10/2001[668]). En esta línea se pronunció el Tribunal Superior de Colonia[669], que no admitió como prueba un correo electrónico firmado con el nombre del demandante, por suponer que el uso del correo electrónico está al alcance de cualquiera y, con ello, puede suponerse lo mismo del uso de la firma electrónica simple.

De esta forma, de acuerdo con el § 126 del Código Civil alemán, cualquier documento o declaración de intenciones deberá tener una firma electrónica reconocida, cuando la Ley establezca la forma escrita. Se dice firma electrónica reconocida, no firma electrónica simple, ya que ésta no cumple los requisitos técnicos de aquella. Además, para que pueda ser considerada una firma electrónica, como pruebas documental de un contrato, tiene que llevar aparejado un certificado reconocido, de acuerdo con el § 371 del Código de Procedimiento Civil alemán. Sin embargo, se prevé que cuando la ley no requiere que un contrato se realice por escrito, las partes pueden acordar el uso de una firma electrónica distinta de la firma electrónica reconocida, debiendo ir acompañadas de pruebas que la hagan indubitable[670].

También, en Alemania, ha habido debate en torno a la utilización de imágenes escaneadas, de la firma de los abogados, con el fin de autenticar escritos de recursos transmitidos por módem, directamente, desde una computadora a la máquina de fax del Tribunal. La Sala Conjunta de los Tribunales Federales Superiores determinó que los escritos obligatorios pueden ser transmitidos por vía electrónica, a través de un archivo de texto con la firma escaneada. Se observó que en las actuaciones judiciales, el requisito de forma, no era un fin en sí mismo. Su finalidad es garantizar una determinación suficientemente fiable (*hinreichend zuverlässig*) del contenido del escrito y la identidad de la persona de la que emana. La Sala Conjunta tomó nota de la evolución práctica de los requisitos de forma, para dar cabida a los adelantos tecnológicos. De esta forma, sostuvo que aceptar ciertas presentaciones procesales, por medio de la comunicación electrónica de un mensaje de datos, en que constara la

[668] ALEMANIA: Sentencia del Tribunal de AG Bonn de 25 de octubre de 2001**,** número de caso 3 C 193/01.
[669] ALEMANIA: Sentencia del Tribunal Superior de Colonia, de 6 de septiembre de 2002, número de caso 19 U 16/02.
[670] ALEMANIA: Sentencia del Tribunal de AG Ettlingen de 11 de mayo de 2001, Caso Nº 2 C 259/00.

imagen escaneada de una firma, concordaría con el espíritu de la jurisprudencia existente[671].

En este punto, llama la atención el criterio que adoptó el Juzgado de lo Civil de *Mondovi*, en Sentencia de 7 de junio de 2004, que confirmó los argumentos del abogado de la parte demandante, que dijo: "para constituir una firma electrónica, los datos deben estar conectados, lógicamente a otro conjunto de datos, que se utilizan como método de autenticación. En Internet, el sistema más simple y más utilizado es la inserción del nombre de usuario y una contraseña es el e-mail, que el usuario debe escribir para autenticar y obtener acceso a un área reservada. Esto sucede con los e-mails: obtener acceso a una cuenta de correo electrónico (es decir, el área reservada que corresponde a una dirección dada como abcdefg@yahoo.it utilizado por el demandado) para enviar o leer mensajes de correo electrónico, se necesita tener conocimiento de estos datos (o utilizar el software, tales como *Microsoft Outlook Express*) en ejecución del procedimiento de validación electrónica. El conjunto de datos de la dirección del remitente (que se inserta en el e-mail, en el momento que se envía, como si fuera un sello) demuestra que el e-mail, en cuestión, fue escrito por alguien que obtuvo acceso a la zona reservada, utilizando un nombre de usuario y una contraseña o, más precisamente, se da fe de que la persona que escribió que el e-mail debe haber insertado un nombre de usuario y una contraseña. Por lo tanto, gracias a la primera serie de datos, se sabe que se utiliza un segundo conjunto de datos, como un método de autenticación, para enviar el correo electrónico y que este segundo conjunto está conectado, lógicamente, con los primeros. En vista de lo anterior, es indiscutible que los e-mails (incluyendo el que se presenta como prueba) constituyen documentos electrónicos firmados con una firma electrónica, tal como se define en el Artículo 1, párrafo primero, inciso cc y 10, párrafo 2, del Decreto Presidencial 445/2000, confirmado recientemente por la jurisprudencia Tribunal de Cuneo, 15 de diciembre de 2003, n ° 848"[672].

[671] ALEMAIA: Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 de abril de 2000, *JurPC Internet- für Zeitschrift Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 160/2000. Disponible en http://www.jurpc.de/rechtspr/20000160.htm (última visita 14/3/2014).

[672] COPPOLA, G.P.: "Italy: Tribunale Mondovi, 7 giugno 2004, n. 375 (decr.), giur. it. 2005, 1026" *Digital evidence and electronic signature law review*, octubre, 2007, núm. 4, págs.86 – 88.

En resumen, el Tribunal, en la Sentencia mencionada, establece que la dirección de correo es un documento electrónico firmado con firma electrónica simple, ya que "el emisor, con el fin de crear y enviar este e-mail, debe realizar una validación mediante la introducción de su nombre de usuario y la contraseña". Esto lo hace basándose en lo siguiente: "El e-mail es un documento electrónico válido y pertinente, para todos los efectos de la Ley; el documento electrónico, si se firma con la firma electrónica cumple con el requisito legal de que sea considerado escrito; el correo electrónico es el documento firmado mediante firma electrónica, ya que el emisor, con el fin de crear y enviar el mensaje, debe realizar una validación; es decir, la inclusión de su nombre de usuario y la contraseña; por tanto, en un mandamiento judicial, la prueba puede quedar determinada por la producción de e-mail".

Esta Sentencia ha sido muy criticada por la doctrina, que entiende que la conexión lógica, que debe existir entre los dos conjuntos de datos, implica que el segundo conjunto autentica la primera, en la que se validan los datos y hace que cualquier cambio posterior detectable. Esto no ocurre cuando se obtiene acceso a un servicio de correo electrónico, ya sea basado en la web o ya en el cliente. El usuario accede al servicio utilizando una identificación de usuario y contraseña, al realizar esta acción, el usuario lo que está efectuado es obtener acceso al servicio. La identificación de usuario y la contraseña no autentica el contenido del correo electrónico enviado a través de este servicio. Si bien este es un argumento legal sutil y técnico, puede tener consecuencias importantes. Una serie de decisiones basadas en los mismos motivos se han publicado recientemente, todas ellos se refieren a juicios sumarios y, por lo tanto, no explican las razones subyacentes. Sin embargo, dado el creciente número de movimientos basados en este tipo de pruebas, es inevitable que los juicios sigan un razonamiento más detallado e instructivo.

Vista la jurisprudencia, se aprecia que en los casos en los que la firma manuscrita no es un requisito, la firma electrónica se puede utilizar como una cuestión probatoria de la conducta o la intención las partes, atendiendo a los términos del acuerdo suscrito. En otras palabras, a pesar de usar una firma electrónica simple, ésta puede ser considerada equivalente a la firma manuscrita o podría ser utilizada como prueba por

una de las partes, ya que podría demostrar la intención real de que la otra parte quería firmar dicho acuerdo, ante la falta del requisito de firmas manuscritas equivalente.

Los requisitos de validez jurídica, en el comercio electrónico, son muy diferentes de los de seguridad del negocio y la confusión, entre los dos, ha llevado, a veces, a aplicaciones inapropiadas de la tecnología, que han terminado por llevar a una falta de interoperabilidad legislativa[673].

Por consiguiente, incidiendo en el error que lleva la regulación tecnológica de la firma electrónica y relacionando la forma simple con la digital, cuando hemos contactado con empresas, nos han constatado que no suelen incurrir en riesgos con partes en las que no confían. Consideran que es necesario apreciar las fuentes de confianza, que subyace en un entorno comercial ya establecido. Esto, nos ha llevado a pensar que la confianza en el comercio electrónico no es una cuestión de fe, de regulación o de tecnología, sino que es el resultado de la gestión de relaciones.

El desarrollo de las relaciones comerciales se deriva de las interacciones de negocios tradicionales, que implican una gama de diversas fuentes y tipos de información complementaria acerca de la otra parte, incluyendo; por ejemplo, reuniones (suelen concretarse por correo electrónico), llamadas telefónicas, correos electrónicos, verificación de crédito y redes.

La idea de una firma electrónica, en nuestra opinión, no necesitaba una nueva definición específica, de manera que el papel a desarrollar, por la firma, tiene que ser igual que antes. La gestión del riesgo, resulta más importante que la autenticación del origen, el destino o la integridad de la documentación, determinando el requisito de vincular el documento, exclusivamente, con la intención de autorizarlo. Este hecho, quizás, pueda requerir mayor cantidad de información acerca de la persona que firma y de su intención, para mayor fiabilidad/seguridad del proceso. Aun así, una cosa esta clara, respecto de la gestión de los riesgos en general, el nivel de autenticación debe ser proporcional al riesgo que implica.

[673] FORDER, J.: "The inadequate legislative response to e-signatures", *Computer Law and Security Review*, Julio, 2010, Vol. 26, núm. 4, págs. 418 – 426.

De esta forma, como hemos visto, los criterios legislativos, que han adoptado las Leyes respecto de la firma electrónica y su autenticación, han influido en la actitud de los Tribunales al respecto. Las Leyes sobre firma electrónica, sin una norma general relativa a la autoría, han hecho que se preste demasiada atención a la función de los métodos de autenticación relativa a la identidad[674], este es el motivo, entre otros, por el que surge, en la Unión Europea, el nuevo Reglamento sobre identificación electrónica.

Ante esta situación, resulta claro que todavía no hay mucha jurisprudencia sobre la firma electrónica y los pocos pronunciamientos judiciales, hasta ahora, no constituyen una base suficiente para fijar criterios sobre el reconocimiento internacional de la firma electrónica.

En cualquier caso, las Sentencias, a los que hemos hecho referencia, muestran que, en la actualidad, no existe ninguna ley clara y coherente que interprete lo que se entiende por firma electrónica. En caso de la UE, en relación con la validez jurídica y la obligatoriedad de la firma electrónica simple, algunos jueces aceptan la validez de ciertas firmas electrónicas, que son, por muchos, consideradas inseguras, tales como las firmas manuscritas escaneadas o la introducción de un nombre en un correo electrónico; otros jueces aceptan que introducir un código PIN equivale a una firma manuscrita.

Así, pensamos, viendo la situación legislativa europea, con la Directiva (y a la espera de la puesta en práctica del nuevo Reglamento), ante la "definición" poco clara del término firma electrónica en el Artículo 2,1, que utiliza términos no definidos (por ejemplo, "autenticación"), abre el debate sobre, en qué medida, si esta firma, puede ser considerada como una firma electrónica legalmente válida. Los Jueces tienen que interpretar lo que debe entenderse por firma electrónica, a pesar de tener dificultades para comprender la forma de evaluar el cumplimiento de los criterios técnicos para la creación de una firma electrónica legalmente válida, ante los diferentes niveles de la firma electrónica (firma electrónica básica, la firma electrónica avanzada , la firma electrónica reconocida).

[674] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 109.

Por este motivo, hay que reconocer que el comercio electrónico se encuentra todavía en una etapa temprana de desarrollo, antes de que se establezca como meta el reconocimiento en la escena internacional. Sin embargo, a pesar de que las Leyes nacionales no están, en este momento, en condiciones de ir tan lejos como para exigir el reconocimiento de firmas y documentos electrónicos en lugar de las formas manuscritas. Esto no significa que haya un impedimento para que los Tribunales reconozcan el uso electrónico de documentos en estos asuntos, bajo la base de caso por caso[675]. Cuando la confianza en las transacciones electrónicas crezca, la Ley puede y, de hecho, será ampliada, para incluir la validez de todo el tipo de firma electrónica, para cualquier documento y cualquier transacción.

5.3. Reconocimiento transfronterizo de la firma electrónica digital[676]

Hay países, que han dado un trato tecnológico a sus leyes: comienzan recogiendo una firma electrónica tecnológicamente neutral, para terminar estableciendo, una especial atención, a las firmas electrónicas digitales. Estas firmas digitales son tecnológicamente específicas, que se crean usando un sistema de criptografía asimétrica o de clave pública.

Este tipo de firmas son consideradas seguras, por cuanto permiten satisfacer, en principio, las exigencias de autoría e integridad necesarias para que el mensaje y su firma electrónica sean vinculantes, para el firmante y exigibles ante los Tribunales e, incluso, es posible que determinados criptosistemas de clave pública puedan ser utilizados para obtener confidencialidad[677].

La actividad regulatoria se desarrolla en favor de las firmas electrónicas digitales, a las que se le añaden determinados requisitos de forma. Como ha señalado el Prof.

[675] SINGAPUR: Joseph Mathew y Otro v Singh Chiranjeev (y Otro [2009] ASGC 51, de fecha de 29 de octubre de 2009).
[676] Nos hemos centrado en la firma electrónica digital basada en la tecnología PKI por ser la tecnología más utilizada, en tanto que países de todo el mundo han aprobado leyes que soportan este tipo de firmas como medio de autenticar datos y transacciones electrónicas. No obstante, en todo lo que nos vamos a referir a esta tecnología, cualquier conclusión que se pueda sacar puede aplicarse a cualquier tecnología.
[677] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de* certificación, Madrid, 2000, pág. 42.

Mason[678], lo que se vienen a establecer en estas legislaciones no son definiciones, propiamente dichas, de la firma electrónica digital, sino un número de características en relación con el rendimiento que se pretende tener de ellas. De esta forma, vienen a establecerse un modelo de seguridad basado en una tecnología determinada (como por ejemplo, Anexo II de la Directiva). A esto hay que añadirles otras exigencias para determinados contratos, en los que es necesaria la intervención de un fedatario público y el registro del contrato[679].

De este modo, se puede afirmar que: el diseño de estas Leyes se ha llevado a cabo en torno a las firmas digitales, haciendo girar la equivalencia formal de las firmas electrónicas entorno a su seguridad, priorizando este principio sobre la neutralidad tecnológica, de tal forma que se viene a dejar un vacío regulatorio en contra de las firmas electrónicas simples, limitándose a establecer que no se le negará validez por el hecho de estar en formato electrónico, dejando al arbitrio de los Tribunales de cada Estado la admisión de estas.

En este trato preferencial dado a las firmas digitales, en términos generales, todas las leyes presentan una estructura similar[680]:

a) Efectos jurídicos: como cuál debe ser el efecto del documento firmado digitalmente, si ese documento firmado digitalmente es equivalente a la firma manuscrita y asignación de requisitos; cuál es su papel como pruebas y otros requisitos o las preferencias respecto a los documentos originales, a efectos de determinar si se presume auténtica y con fines probatorios, etc.

b) Establecen artículos que se refieren al propio "reconocimiento de certificados extranjeros", recogiendo requisitos para determinar su validez.

c) Establecen presunciones; por ejemplo, que la firma digital es tan buena como una firma escrita a mano, sólo si la firma digital es verificada por referencia a

[678] MANSON, S.: *Electronic signature in Law,* Cambridge, 2011, pág. 161 y ss.
[679] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 109.
[680] CAROLINA, R; LYFORD, J; LYONS, T.*:* "The Intersection of Public Key Infrastructures and the Law", *Information Security Technical Report*, 2000, vol. 5, nº 4, págs. 39 – 52.

un certificado emitido por un tercero de confianza, éste solo puede ser fiable si el usuario puede confiar en el emisor del certificado, etc.

d) Establecen límites de responsabilidad, se incluyen ciertos límites destinados a restringir el derecho de las partes, a confiar en los certificados, y el derecho a recuperar del emisor las pérdidas sufridas, como resultado de la confianza.

e) Establecen la responsabilidad, casi siempre, en exclusiva del tercero en confianza, que emite el certificado, no recogiendo los derechos y obligaciones comunes de los participantes en la transacción, realizada a través de la infraestructura PKI.

Con esta estructura, se observa que las Leyes, que han establecido la tecnología PKI, se han basado en el Derecho para establecer una mínima coincidencia, en el establecimiento de los derechos y deberes entre usuarios, lo que no tiene por qué llevar a la denegación del reconocimiento legal de las firmas o certificados extranjeros.

No obstante, a pesar de la existencia de este mínimo coincidente, las legislaciones varían en el establecimiento de los requisitos formales de los actos jurídicos y en las consecuencias jurídicas de la transacción, hasta el punto de que tener una firma digital no es suficiente para su reconocimiento. Lo que nos lleva a confirmar el carácter discriminatorio y excluyente de las Leyes.

El sistema es complejo, ya que la infraestructura implica tener un mensaje o documento del emisor, que aplica una firma digital a un mensaje en el contexto en el que, un tercero verifica la identidad del firmante (y que también podrá emitir y controlar la firma digital), mediante la emisión de un certificado que confirma que el componente de clave pública fue emitida por el firmante y que éste tiene la clave privada en lo que se conoce como una infraestructura de clave pública o PKI[681].

[681] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 43 y ss.

Esto se puede complicar aún más, en el papel de certificación de la Autoridad Certificadora, que incluirá en el certificado de la firma digital, mediante su propia clave privada para garantizar, tanto integridad del mensaje y como la autenticidad de la identidad. En el proceso de certificación, para garantizar la autenticidad de cualquier mensaje, pueden estar involucradas varias entidades emisoras de certificados[682]. De esta manera, el papel de estas entidades emisoras se complica en el reparto y la gestión de la responsabilidad. Esto trasladado a un contexto internacional, se complica por la falta de seguridad jurídica ante la falta de un marco legal consensuado.

Las firmas digitales pueden ser ejecutadas en casi todos los países. Sin embargo, a menudo es difícil de cumplir con la tecnología y requisitos de seguridad de cada jurisdicción; pues, no existe un sólo tipo de tecnología PKI[683], lo que nos lleva a observar, además de un problema de autenticación de certificados, un problema de distribución e integración de los mismos.

Los sistemas estándares de PKI incluyen componentes múltiples: la autoridad certificadora, dispositivo del almacenaje de claves (hardware o software), software para la gestión de claves, para gestión e incorporación de nuevos usuarios y, por supuesto, los componentes necesarios para firmar en aplicaciones de la vida real (aplicaciones de workflow, ERP, correo, o cualquier otra). La integración de todos estos componentes es compleja y muy costosa de mantener en el día a día.

Hasta hace poco tiempo, ha habido pocas alternativas estándares de interconexión entre los diversos componentes, y aun poniendo estos interfaces en marcha, cada vendedor define su propia versión del interfaz. Esto ha creado procesos largos y costosos de integración, donde los costes han aumentado. La integración de la infraestructura de firma digital con las aplicaciones es compleja e implica generalmente desarrollos, utilizando API criptográficos a bajo nivel. Aunque la tecnología está madurando y los vendedores cada vez cumplen más los estándares de la industria, la única manera de interaccionar, con los tokens (hardware o software) y con la autoridades de certificación es a través de estos interfaces criptográficos de bajo nivel

[682] COUTO CALVIÑO, R: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista Electrónica de la Contratación*, núm. 83, junio, 2007, págs.. 3 – 37.
[683] SALLINGS, W.: *Fundamentos de Seguridad en Redes: Aplicaciones y Estándares*, Madrid, 2004, págs. 55 y ss.

(tales como PKCS#11, y MS-CAPI), que requieren un profundo conocimiento de la tecnología PKI[684].

Ante la dimensión internacional que tienen las comunicaciones comerciales electrónicas, se hace necesario un trabajo común, para crear medios de seguridad, que sean estándares para todos y llegar a una normalización en los sistemas de firma electrónica, que permitan, no sólo presentar documentos en nuestra Administración electrónica, sino también cerrar operaciones electrónicas, con cualquier prestador de servicios, que se encuentre en cualquier país del mundo; pues ¿de qué nos sirve un sistema de firma electrónica, cuando este requiere de su uso por la otra parte contratante y esta no la tiene implantada o el sistema de firma electrónica que tiene implantado no es compatible con el nuestro?[685].

Asimismo, somos conscientes de que el comercio electrónico funciona; o sea, constantemente se realizan compras de bienes y servicios en Internet; pero, en la gran mayoría de los casos, con otros tipos de firma electrónica (por ejemplo, pulsando el icono de "Acepto" o escribiendo un nombre en un mensaje de e-mail). La firma electrónica digital parece que cada vez tiene menos uso, a pesar de la ingente regulación que se ha promulgado en los distintos países. No obstante, siempre hay una excepción, como veremos más adelante[686]: la administración electrónica.

5.3.1. El papel de las autoridades de certificación

Cualquier sistema legal de firmas digitales requiere la intervención de una o más terceras partes de confianza, que emiten certificados que, a la vez, sirven para distribuir la clave pública, para asociar de forma segura la identidad de una persona concreta. La tercera parte de confianza desempeña de forma, fundamental, la función de emisión de certificados. La principal función del certificado emitido es unir un par de claves con la firma de una determinada persona. El destinatario de un certificado que desee confiar y

[684] LEVIN, R.: RESNITZKY, U.: "El libro blanco de la Firma Digital: la mejor aproximación a la firma digital basada en PKI", *Arx: Algorithic Research*, enero, 2005, págs.1 – 15.
[685] ARIAS POU, Mª: *Manual práctico de comercio electrónico*, Madrid, 2006, pág. 469.
[686] SCHAPPER, P. R.; RIVOLTA, M.; LEIPOLD, K.: "Authentication: International scope and non discrimination in government commerce vs. PKI", *Digital evidence and electronic signature law review*, núm 2, octubre, 2005, págs. 55 – 61.

apoyarse en una firma digital, creada por el suscriptor, puede usar la clave pública incluida en el certificado, para verificar que la firma digital fue creada con la correspondiente clave privada[687].

El problema surge a la hora de hacer frente a la aceptación de certificados digitales a nivel transfronterizo; pues, el comercio electrónico, a menudo, cruza los límites jurisdiccionales y las partes intervinientes en una transacción pueden tener certificados digitales diferentes, de entidades emisoras diferentes y cada una de estas entidades, según el Estado en el que estén domiciliadas, tendrá reglas diferentes. Ante esta situación, la armonización de las normas técnicas, los procesos de negocio y los marcos legales resultan de vital importancia, para el reconocimiento de estas firmas electrónicas.

Si no hay reconocimiento de los certificados o firmas digitales, el papel de estas firmas puede quedar seriamente afectado[688]. Además de tratar los temas legales de reconocimiento transfronterizo, la autoridad certificadora, también debe hacer frente a las consideraciones técnicas, como la compatibilidad de software y procedimientos viables para aceptar y evaluar los certificados emitidos por otras autoridades de certificación[689].

En este punto, es necesario acudir a la Ley Modelo sobre Firma Electrónica que en su Artículo 12, intitulado "el reconocimiento de certificados y firma electrónica", nos lleva a una posible solución, al establecer el principio de no discriminación, tratando de dar validez jurídica a una firma o certificado, con independencia de donde se haya expedido, siendo su fiabilidad técnica[690] el factor que determine su efecto jurídico; pues, de nada serviría si no se estableciera una pauta aceptable, segura y difundida en materia

[687] MARTÍNEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, págs. 65 y 66.
[688] SRIVASTAVA, A.: "Electronic signatures and security issues: An empirical study", *Computer Law & Security Review*, septiembre, 2009, vol. 25, núm.5, págs. 432 – 446.
[689] MASON, S.: "Electronic Signatures - Evidence: the evidential issues relating to electronic signatures", *Computer Law & Security Review*, mayo, 2002, vol. 18, núm. 3, págs.. 175 – 180.
[690] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 145.

de reconocimiento, en el país del foro de la firma electrónica o del certificado que la acompañe[691].

El origen es un factor clásico dentro del marco del Derecho Internacional, es la base del criterio de reciprocidad; es decir, con él se le da valor jurídico a una firma electrónica en el ámbito de un país determinado, siempre que otro país le dé el mismo valor a las de aquél[692].

Este grado de fiabilidad es referido, por la Ley Modelo sobre Firma Electrónica, para establecer un criterio que dé seguridad jurídica, para su reconocimiento transfronterizo, estableciendo un criterio de equivalencia técnica que impida la discriminación, que podría darse en caso contrario y que, como veremos más adelante, se produce de manera efectiva, dándose preferencia, en la mayoría de los casos a los prestadores de servicios de certificación nacionales sobre cualquier otro extranjero.

De esta manera, el principio de equivalencia sustancial del nivel de fiabilidad debe ser distinto según los tipos de certificados existentes, pero en igualdad de condiciones[693]. Sin embargo, se hace depender de lo dispuesto en los estándares reconocidos a nivel internacional o en otros factores relevantes sin ulteriores precisiones, lo que limita la eficacia práctica de la norma[694].

La fiabilidad, y con ella su equivalencia, llevará a comprobar qué certificados son comparables o, lo que es lo mismo, qué certificados tienen un mismo nivel, siendo el Tribunal del Estado donde se dirima la controversia, quien tendrá que resolver el efecto que producirá el certificado extranjero, estableciendo la posible y adecuada correspondencia con el nacional[695].

---

[691] MADRID PARRA, A: "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Derecho Patrimonial*, año 2003 – 2, número 11, págs. 31 - 63.
[692] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 175.
[693] MADRID PARRA, A: "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Derecho Patrimonial*, año 2003 – 2, número 11, págs. 31 - 63.
[694] MIGUEL ASENSIO, P.A.: Derecho Privado de Internet. Madrid, 2002, pág. 419.
[695] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMCE*, párr. 153: en referencia la párrafo 2 del artículo 12: "establece un umbral de equivalencia técnica de los certificados extranjeros basados en contrastar su fiabilidad con los requisitos de fiabilidad establecidos por el Estado promulgante, de conformidad con la Ley Modelo. Este criterio ha de aplicarse

Pueden plantearse varios problemas, con respecto al reconocimiento de certificados por las autoridades de certificación de países extranjeros. Hoy en día, el reconocimiento de certificados extranjeros se realiza a menudo mediante el método llamado: "certificación recíproca", el caso en el que autoridades de certificación, equivalentes, reconocen los servicios prestados por cada cual, de tal manera que sus usuarios respectivos puedan comunicarse entre sí, con mayor eficacia y más confianza en la fiabilidad del certificado que se expida[696]. Se destaca:

a) El reconocimiento recíproco: es un arreglo de interoperabilidad, en virtud del cual cada parte que confía y que se encuentre en la zona abarcada por una ICP, puede utilizar la información autorizada correspondiente a la zona de cobertura de otra ICP, para autenticar datos en la zona abarcada por la primera ICP. A los efectos de reconocimiento recíproco, la decisión de confiar en un certificado extranjero, corresponde a la parte que confía y no a su prestador de servicios de certificación[697].

b) La certificación recíproca entre infraestructuras de clave pública: es la práctica de reconocer la clave pública de servicios de referencia a un nivel convenido de confianza, habitualmente, en virtud de un contrato. Básicamente da lugar a que dos dominios de ICP se fusionen en uno mayor[698].

En lo que se refiere a este reconocimiento recíproco, la carga suplementaria que imponen al prestador de servicios de certificación extranjero los requisitos nacionales, determinados por la tecnología, que pueden convertirse en obstáculo al comercio internacional[699]. De esta manera, se han promulgado Leyes relativas a los medios por

---

prescindiendo de la naturaleza del sistema de certificación utilizado en la jurisdicción de donde emanó el certificado o la firma".

[696] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 164.

[697] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 167 y ss.

[698] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 169y ss.

[699] ALLIANCE FOR GLOBAL BUSINESS: *A discussion paper on trade-related aspects of electronic commerce in response to the WTO´s e-commerce work programme*, abril, 1999, págs. 29 y 30. Disponible en: http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf (última visita: 20/3/2014)

los que las autoridades de certificación reconocen firmas y certificados extranjeros, lo cual llega a constituir una discriminación en contra de las empresas extranjeras[700].

Estas legislaciones, que únicamente consideran válidas las firmas electrónicas, basadas en un certificado emitido por un prestador de servicios de certificación autorizado para operar en el foro, son ineficaces al imponer una restricción que, a largo plazo, menoscaba la posición competitiva y el comercio internacional, generando incertidumbre[701].

Todos los países, que han examinado esta cuestión, han incluido en el articulado de sus leyes de firma electrónica, alguna alusión relativa al prestador de servicios de certificación extranjero; por lo que esta cuestión se encuentra ligada a las posibles diferencias entre las normas vigentes en los países[702]. Al mismo tiempo, las legislaciones han impuesto otras limitaciones geográficas o procedimientos, que impiden el reconocimiento transfronterizo de las firmas electrónicas.

En definitiva, la divergencia de normativa, que se ha dado de forma generalizada, ha sido resultado del establecimiento, por determinados países, de requisitos más estrictos y particularizados para las firmas (como por ejemplo, la UE[703]), mientras otros países se centran en la intención de la parte firmante y establecen, en sus ordenamientos, una extensa variedad de formas de probar la validez de las firmas (como por ejemplo, Estados Unidos[704]).

Esto se debe principalmente al diferente concepto de firma que cada Estado establece en su propio Ordenamiento Jurídico. Por un lado, es la manifestación del principio de equivalencia funcional, como instrumento electrónico, que identifica al firmante e indica que éste aprueba el contenido del mismo; y por otro, se establecen, en los ordenamientos, elementos tecnológicos, que suponen la ruptura con el principio de

[700] Por ejemplo, el Art. 14 de la Ley 59/2003, de 9 de Diciembre, transposición literal del Art. 7,1 de la Directiva 1999/93/CE de Firma Electrónica.
[701] MIGUEL ASENSIO, P.A.: "Regulación de la firma electrónica: balance y perspectiva", *Direito da Sociedade da Informaçao, Coímbra*, 2004, págs. 115 – 143.
[702] CAROLINA, R; LYFORD, J; LYONS, T.: "THE Intersection of Public Key Infrastructures and the Law", *Information Security Technical Report*, 2000, vol. 5, nº 4, págs. 39 – 52.
[703] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
[704] Electronic Signature in Global and Nacional Commerce Act (E-Sign), 30 de julio de 2000.

neutralidad tecnológica, que hacen que este principio quede supeditado a la equivalencia funcional.

Este escollo conceptual quedaría solucionado, si en dicho concepto de firma, se apelara a que ambos principios se situarán en un mismo nivel; es decir, sin restricción de una tecnología y al cumplimiento, de pleno, de las funciones, que debe cumplir una firma electrónica[705].

Por otro lado, Artículo 12,4 de la Ley Modelo, nos dice que "para evaluar la equivalencia de los certificados se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente", factores enumerados en los Artículos 6, que recoge el fundamento de la Ley Modelo; Artículo 9 que trata el sujeto esencial para que entre en juego la firma electrónica: el prestador de servicios de certificación o autoridad de certificación; y Artículo 10, que en conexión con el anterior, recoge la fiabilidad de los medios, sistemas y procedimientos para "apoyar" una firma electrónica.

En cualquier caso, la falta del valor jurídico necesario de la Ley Modelo provoca limitación en la eficacia práctica de la norma. No obstante, cabe la posibilidad de que las partes se pongan de acuerdo, sobre el reconocimiento de la eficacia transfronteriza de ciertas categorías de certificados o de firmas, tal y como se reconoce en el Artículo 12,5 de la propia Ley Modelo, siempre que esos acuerdos no se hallen prohibidos o carezcan de eficacia, conforme a la ley aplicable[706].

Asimismo, prevé el acuerdo entre las partes como suficiente para el reconocimiento transfronterizo de una firma electrónica, siendo importante para ello dar efecto a las estipulaciones contractuales, conforme a las cuales podrán convenir dicho reconocimiento en el uso de firmas electrónicas o certificados, recurriendo a la

[705] CRUZ RIVERO, D.: *Eficacia Formal y Probatoria de la Firma Electrónica*, Madrid, 2006, pág. 50. Recoge las funciones que debe cumplir una firma dentro del principio de equivalencia funcional. "lo que exige un signo electrónico para ser considerado firma es su capacidad para autentificar un documento, para suscribir y mostrar la identidad del suscriptor. Por lo tanto si la LEF (interpretada a la luz de la DFE) establece que la función que debe cumplir una firma electrónica para considerarse tal es la autentificación, no debe añadirse ninguna otra función de la firma manuscrita".
[706] MIGUEL ASENSIO, P.M.: *Derecho privado de Internet*, Madrid, 2002, pág. 419.

autonomía de la voluntad de las partes, como motivo suficiente para el reconocimiento transfronterizo.

El principio de autonomía de la voluntad se repite en el Artículo 5 de la Ley Modelo, lo hace refiriéndose a que siempre es posible que las partes pacten, entre sí, el reconocimiento de determinados certificados o firmas electrónicas, reuniendo la validez que establezca el Derecho aplicable para cada acuerdo[707].

Sin embargo, este reconocimiento nos lleva a otro problema, que será tratado en su momento: la cuestión de la responsabilidad, que puedan corresponder a cada una de las partes interesadas, en el funcionamiento de los sistemas de creación de firmas electrónicas; pues, las legislaciones nacionales fijan diferentes criterios para evaluar las distintas formas de actuar y, además, establecen regímenes de conducta y los requisitos del certificado. Como es lógico, si se incumplen las pautas de conducta establecidas, se incurrire en responsabilidad.

En resumen, el panorama que nos encontramos, para hacer frente a la eficacia transfronteriza de los certificados, ofrece una gran variedad de legislaciones, que más que facilitar el uso de la firma electrónica, la obstaculiza, creando incertidumbre y ausencia de criterios comunes, que permitan establecer un régimen uniforme.

Ante esta situación planteada, observamos, esencialmente, tres vías en el reconocimiento de las firmas electrónicas y sus certificados: la primera, el Estado en el que se integra el prestador de servicios de certificación, que emite el certificado, y, por tanto, pretende hacer valer que su certificado forme parte de un marco jurídico integrador, que permita adecuar las legislaciones nacionales, con el fin de eliminar cualquier obstáculo, que pueda ser fijado en ellas, de manera que pueda garantizarse la eficacia, en todos los Estados miembros, los certificados emitidos. Con ello, nos estamos refiriendo claramente a la Unión europea.

La segunda, es la posibilidad de que exista entre los territorios implicados, un Tratado o Convenio Internacional, ya sea bilateral o multilateral, que permita fijar las

[707] MADRID PARRA, A: "Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Derecho patrimonial*, año 2003 – 2, número 11, págs. 31 - 63.

condiciones bajo las que puede tener lugar el reconocimiento reciproco de la eficacia de estos certificados. Esta opción ha sido desarrollada por la CNUDMI a través de la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005.

La tercera vía, presenta la posibilidad de que un Estado establezca un régimen, que haga posible la eficacia en el foro de los certificados expedidos por entidades de certificación extranjera, acorde a lo establecido en el Artículo 12 de la Ley Modelo sobre Firma Electrónica; el ejemplo, lo encontramos en la legislación de Estado Unidos.

No obstante, puede producirse ese reconocimiento de los certificados en el foro, pero bajo ciertos controles, que vienen a obstaculizar el propio reconocimiento transfronterizo. Estos controles pueden centrarse bien en el prestador de servicios de certificación o bien en el certificado expedido.

De esta manera, cuando el control va referido al prestador de servicios, se admite la eficacia de sus certificados si éste satisface los requisitos impuestos en la normativa del foro, para ese tipo de entidades y esta circunstancia ha sido verificada, por un organismo de supervisión del foro, ante el que se ha solicitado la pertinente acreditación (por ejemplo, Singapur)[708]. Cuando se trata de controlar directamente los certificados, cuya equivalencia de efectos con los de las entidades en el foro en el que se pretende hacer valer el certificado, suele resultar determinante que el certificado cumpla los requisitos exigidos en el foro y éste sea avalado por un prestador de servicios local acreditado, solución[709] que se vincula con los conocidos como acuerdos de certificación recíproca[710].

5.3.2. Reconocimiento de los certificados extranjeros

La característica común de los Estados, que dan un trato preferencial a la firma digital, es que establecer en sus Leyes, artículos que se refieren de manera expresa, al

[708] MASON, S.: *Electronic signature in Law,* Cambridge, 2011, pág. 176.
[709] Esta solución, en referencia a los tipos de controles que se realizan directamente sobre los certificados, la encontrábamos en el Artículo 7 de la Directiva 1999/93/CE y han desaparecido con el Reglamento 910/2014.
[710] MIGUEL ASENSIO, P.M.: *Derecho privado de Internet*, Madrid, 2002, pág. 418.

reconocimiento de certificados extranjeros[711]. Estos artículos exigen determinadas condiciones, que deben cumplir los certificados digitales; pues, de no cumplirse éstas se les negarán cualquier posible eficacia legal.

Debemos tener en cuenta que un certificado, de forma genérica y descriptiva, es un documento electrónico, que contiene una información a la que se ha fijado una firma digital por alguna entidad, que es reconocida y en la que confía alguna comunidad de usuarios de certificados. Dentro de este concepto, caben diversos tipos de certificados, que pueden servir para distintas finalidades. El tipo de certificado más importante es el certificado de clave pública[712].

La función básica del certificado es vincular una clave pública con una persona determinada, autenticar la titularidad de la clave pública y comprobar la identidad del firmante, lo que planteará la cuestión de responsabilidad del proveedor, en caso de emisión de certificados falsos. Así lo entiende, la CNUDMI, que en la Ley Modelo sobre Firma Electrónica, en el Artículo 2 apartado b), nos dice que por certificado "se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre el firmante y los datos de creación de la firma". Al mismo tiempo, en este mismo Artículo, en el apartado e), nos dice que se entenderá por prestador de servicios de certificación a "la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas".

Esto nos lleva a relacionar la aplicación y utilización de certificados, necesariamente, con la participación de elementos personales, que en el caso concreto del reconocimiento de certificados, nos conduce al emisor del certificado: la autoridad de certificación. De esta forma, la clave de los artículos de reconocimiento de certificados está en la autoridad de certificación, que es quien los emite.

Por consiguiente, en muchas Leyes se viene a establecer un marco jurídico restrictivo y discriminatorio, que viene a evitar que se lleve a cabo la autenticación

[711] MASON, S.: *Electronic signature in Law,* Cambridge, 2011, pág. 174.
[712] MARTINEZ NADAL, A.: *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 2000, pág. 124.

electrónica de manera práctica y global. Las exigencias legales pueden ser de distintos tipos[713]:

1) Estableciendo directrices, prácticas u otros asuntos que se relacionan con la dotación de infraestructuras de autenticación. Tales que sean reconocidos los certificados por un prestador de servicios de certificación del país donde se pretende hacer valer el certificado, para que avale o garantice la validez y vigencia del certificado[714]. La adopción de este sistema requiere que los requisitos establecidos, para el reconocimiento de certificados extranjeros, se interpreten junto a los requisitos necesarios para el establecimiento del sistema de licencias para las autoridades de certificación; pues, se exige un requisito añadido, la aprobación de la autoridad de la aplicación, es decir, la administración.

2) Instauración obligatoria de estándares nacionales, para los productos y servicios de autenticación electrónica[715]. Así, el proveedor de servicios de certificación debe cumplir los requisitos establecidos en la Ley y, además, quedar acreditado en el marco de un sistema voluntario de acreditación establecido en ese Estado.

3) Creación de un marco para regular la supervisión, acreditación y certificación de algunos o todos los productos y servicios de autenticación; o sea, a través de una acuerdo de reciprocidad o tratado internacional; de esta forma, los certificados emitidos por los proveedores de servicios de certificación extranjeros, tendrán los mismos efectos jurídicos que los emitidos por proveedores de servicios de certificación establecidos en el país, donde se quiera hacer valer el certificado[716].

---

[713] KUNER, C; BARCELO, R; BARKER, S.; GREENWALD, E.: *An Analysis of International Electronic and Digital Signature Implementation Initiatives: A Study Prepared for the Internet Law & Policy Forum (ILPF),* A Study Prepared for the Internet Law & Policy Forum (ILPF), septiembre, 2000. Disponible en: http://www.ilpf.org/groups/analysis_IEDSII.htm (visitado en 13-2-2014).

[714] Artículo 16 apartado b) de la Ley de Firma Digital Nº 25506 de Argentina; Artículo 15 de la Ley Nº 19799 de Chile; artículo 7,2 de la Directiva 1999/93/CE.

[715] Artículo 7,2 de la Directiva 1999/93/CE./ Artículo 14, 2 –a) del Reglamento 910/2014.

[716] Artículo 26 de la Ley de China "With approval by the agency in charge of information industries under the State Council in accordance with the relevant protocols or with the principle of reciprocity, certificates of verified electronic signatures issued abroad by foreign electronic verification service

5.4. Reconocimiento de la firma electrónica digital dentro de espacios integrados: especial referencia a la Unión Europea

5.4.1. La equivalencia de los certificados comunitarios

Con la Directiva 1999/93/CE se creó un marco comunitario para el uso de la firma electrónica, estableciendo la libre circulación de productos y servicios de firma electrónica a través de las fronteras, garantizando un reconocimiento jurídico básico de este tipo de firmas.

El objetivo de este marco jurídico era garantizar transacciones electrónicas seguras entre empresas, ciudadanos y administraciones, reforzando la eficacia de los servicios electrónicos, estableciendo un marco regulador para las firmas electrónicas reconocidas, no para las firmas electrónicas más simples a las que, como hemos comentado, se limita a darles validez por el simple hecho de estar en formato electrónico (Artículo 5,1), sin perjuicio de la facultad de los Tribunales nacionales, para dictar resoluciones acerca de la conformidad de los requisitos de la presente Directiva, no afectando a las normas nacionales en lo que se refiere a la libertad de la valoración judicial de las pruebas (Considerando 21)[717]. Surge, así, un problema con las firmas electrónicas simples y con los certificados electrónicos no reconocidos, que será tratado más adelante.

De esta forma, por un lado, se exige a los Estados miembros que garanticen la aceptación de la firma electrónica reconocida, que cumple los requisitos legales de la firma manuscrita y es admisible como prueba en los procedimientos judiciales, de la misma manera que se admite la firma manuscrita en los documentos tradicionales.

Por otro, los Estados miembros no podrán establecer restricciones para los servicios de certificación, que procedan de los Estados miembros del Espacio

---

providers have the same legal effect as those issued by electronic verification service providers authorized by this law"; Artículo 7, 3 de la Directiva 1999/93/CE / Artículo 14, 1 del Reglamento 910/2014.

[717] MASON, S.: *Electronic signature in Law,* Cambridge, 2011, pág. 112.

Económico Europeo, estableciéndose, así, el principio de libre prestación de servicios, a la vez que el principio de equivalencia intracomunitaria de certificados. En principio, este hecho resulta positivo, para el supuesto de los certificados reconocidos sometidos, por imperativo comunitario, a una regulación mínima coincidente[718].

Sin embargo, a pesar de estas exigencias, la armonización conseguida por la Directiva ha sido imperfecta. Se han detectado divergencias en su aplicación a nivel nacional, debido a las diferentes interpretaciones por parte de los Estados miembros, acogiendo *de facto*, excepciones para las aplicaciones del sector público, obsolescencia de las normas, obligaciones de supervisión diferentes y poco claras, que se traducen en problemas de interoperabilidad transfronteriza[719], segmentación y falseamiento del mercado interior[720].

Tal y como puede verse en nuestra Ley 59/2003, sobre firma electrónica, el legislador español, opta por el acceso al mercado de entes del sector público[721], estableciéndose una distorsión de la libre competencia[722], que puede venir, bien por la actuación de un ente público como entidad certificadora, o bien por el establecimiento de especiales requisitos, que exijan las distintas Administraciones públicas[723] para que la firma electrónica surta efectos ante ellas[724]. Estos requisitos o condiciones quedan cumplimentados en el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos, para la sustitución de la aportación de certificados por los ciudadanos.

---

[718] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica*, Madrid, 2009, pág. 267.

[719] Véase, el Capítulo cuarto, la interoperabilidad (págs. 264).

[720] COMISIÓN EUROPEA: *Documento de trabajo de los servicios de la Comisión: resumen de la evaluación de impacto que acompaña al documento de Propuesta del Parlamento Europeo y del Consejo relativo a la identificación electrónica y servicios para la confianza en el mercado interior*, Bruselas, 2012, pág. 3.

[721] Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT, designada por el artículo 84 de la Ley 66/1997, de 30 de diciembre, desarrollada por el Real Decreto 1290/1999, de 23 de julio, para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez, y eficacia de las comunicaciones.
Disponible en: http://www.cert.fnmt.es/index.php?o=legis&lang=es#Inicio (última visita: 3/9/2014).

[722] Resulta un ejemplo de esta distorsión de la libre competencia la Disposición adicional quinta en tanto que declara la exención de la FNMT de la constitución de la garantía del artículo 20,2 Ley 59/2003, de 19 de diciembre, de firma electrónica, es decir, la garantía de 3.000.000 € "para afrontar el riesgo de responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan".

[723] Artículo 4,1 – 2º párrafo de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

[724] MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de la Contratación Electrónica*, Abril, 2001, pág. 35.

Con este reconocimiento se recoger el llamado principio de libre acceso[725], al concretarse la no sujeción de la prestación de servicios de certificación a autorización previa. Este principio abre la vía para que los operadores públicos de servicios de certificación accedan al mercado y compitan con los prestadores privados, con arreglo a los principios de objetividad, transparencia y no discriminación[726].

La no exigencia de autorización previa consagra un sistema, en el que el control de los prestadores de servicios de certificación no *ex ante*, de carácter administrativo, sino *ex post*, de carácter judicial[727]. Además, el legislador, por los servicios que realiza el prestador de servicios de certificación, establece un determinado control y supervisión, a ejecutar por parte de la Administración, articulándose un sistema propio de difusión de información sobre los prestadores que operan en el mercado, certificaciones de calidad y características de los productos y servicios con que cuentan, para el desarrollo de su actividad; es decir, un registro administrativo.

De esta manera, se ha tratado de legitimar la libre circulación en toda la Unión Europea de los servicios de certificación prestados, con independencia de la nacionalidad y del lugar de establecimiento del prestador de servicios de certificación, lo que saca a luz, el problema del reconocimiento transfronterizo en la responsabilidad del propio prestador de servicios, que veremos más adelante en el siguiente capítulo.

En definitiva, se ha intentado optar por un sistema, que descansa sobre la libertad y el voluntarismo del prestador de servicios de certificación y la confianza en el mercado, como mecanismo regulador[728]. Por ello, los prestadores de servicios que "expidan certificados reconocidos al público", en el país en el que se encuentran establecidos, pueden ser equivalentes a los expedidos por los prestadores establecidos en España, apreciándose en rigor la equivalencia de certificados reconocidos.

---

[725] COUTO CALVIÑO, R.: *Servicios de certificación de firma electrónica y libre competencia*, 2008, pág.67.
[726] Artículo 5,3 de la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.
[727] HUERTAS VIESCA, M.I. y RODRÍGUEZ RUÍZ DE VILLA, D.: *Los prestadores de servicios de certificación en la contratación electrónica*, Madrid, 2001, pág. 92.
[728] COUTO CALVIÑO, R.: *Servicios de certificación de firma electrónica y libre competencia*, 2008, pág.72.

Ante esta situación, la Comisión se da cuenta que los Estados miembros han regulado diferentes formatos de firma electrónica, para firmar electrónicamente documentos, que hace que los receptores, que tienen que procesar dichos documentos, encuentren dificultades técnicas, derivadas de la variedad de formatos de firma utilizados[729].

Autoridades públicas de toda Europa han desarrollado el acceso electrónico a sus servicios administrativo, pero lo han hecho centrándose en necesidades y medios nacionales, lo que ha generado un sistema complejo, con soluciones diferentes. Esta situación amenaza con ahondar en los obstáculos, que ya se producen en los intercambios transfronterizos y que lastran el funcionamiento del mercado único, para empresas y ciudadanos.

La Comisión considera que el obstáculo más serio, que dificulta el acceso transfronterizo a los servicios electrónico, es el que se encuentra relacionado con la Administración pública y la posibilidad que ésta ofrece a empresas y ciudadanos que se comunican electrónicamente con ellas[730]. Desde nuestro punto de vista, es totalmente lógico, si tenemos en cuenta que la Administración pública, de un Estado en el que reside una persona, requiere el uso de un determinado tipo de firma electrónica o certificado y la Administración, de otro Estado, requiere otro certificado electrónico para comunicarse con ella, porque no es interoperable con el exigido por la administración receptora, evidentemente dejara de usar el medio electrónico para utilizar el método tradicional en papel, lo que o tendrá un coste doble, por lo que conlleva la duplicidad de certificados electrónicos.

Este fracaso práctico de la firma electrónica reconocida ha supuesto que se considerara mejorar el marco jurídico y administrativo, a fin de liberar el potencial de las empresas, ante la necesidad de definir nuevos objetivos y fijar un nuevo marco de interoperabilidad; pues hasta ahora parecía que la firma electrónica reconocida y el

[729] Considerando 3 de la Decisión de la Comisión por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes de la Directiva 2006/123/CE de Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

[730] COMISIÓN EUROPEA: *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el plan de acción sobre la firma electrónica y la identificación para facilitar la prestación de servicios públicos transfronterizos en el mercado único*, Bruselas, 29 de noviembre de 2008, pág. 3 y 4. (COM (2008) 798 final).

mercado mundial de los servicios electrónicos parecían haber existido, desde hace algún tiempo, cada uno, en realidades paralelas.

En este contexto, se aprueba el Reglamento 910/2014 de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que establece un marco de interoperabilidad, por el que se interconectan los sistemas, la información y los métodos de trabajo. La interoperabilidad de los sistemas de información permite integrar la prestación de servicios en una ventanilla única[731], cualquiera que sea el número de sistemas u organismos administrativos diferentes que intervengan, como pudo observarse cuando a STORK. No se trata solamente de interconectar redes de ordenadores, sino también de abordar cuestiones de organización relativas a la necesidad de garantizar el inter-funcionamiento, con entidades asociadas cuya organización interna y funcionamiento pueden diferir. La instauración de servicios paneuropeos de Administración electrónica pasa, necesariamente, por acuerdos sobre normas y especificaciones comunes. La mayoría de los Estados miembros han abordado esta cuestión, mediante la adopción de acuerdos de colaboración dentro de los "marcos de interoperabilidad para la administración electrónica" nacional, completados por la instauración del marco de interoperabilidad europeo[732].

[731] UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005, pág. 3 y 4 (ECE/ TRADE/352, July 2005).
Disponible en: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf (última visita: 14/3/2014).

[732] Un ejemplo, podemos encontrarlo en España y Portugal que han firmado un Convenio de Colaboración para la prestación de servicios de validación de los certificados electrónicos, **l**os primeros pasos para desarrollar este acuerdo se han dado a nivel técnico**,** De forma recíproca, España garantizará la validación técnica progresiva del Documento Electrónico portugués de identidad (Cartão de Cidadão). En estos momentos la aplicación del Ministerio de Trabajo e Inmigración denominada REA (Registro de Empresas Acreditadas) ya admite el documento de identidad portugués para acreditar que las empresas portuguesas que operan en el sector de la construcción en España cumplen los requisitos de capacidad y de calidad de la prevención de riesgos laborales. Este Convenio de Colaboración, de tres años de duración, abre la posibilidad para que, progresivamente, los servicios electrónicos portugueses sean accesibles con los certificados digitales reconocidos en España en la plataforma @firma, y los servicios electrónicos españoles sean progresivamente accesibles con los certificados digitales portugueses reconocidos por su plataforma de validación.
Disponible en:
http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/MPR/_2010/ntpr20100202_Portugal.htm (última visita: 14/3/2014).

Además, ante las dificultades planteadas, en el marco jurídico de la firma electrónica, el Reglamento regula en los Artículos 25 y siguientes, las normas relativas a la firma electrónica ampliando, el Artículo 5 de la Directiva, estableciendo una obligación explicita de otorgar a las firmas electrónicas cualificadas, los mismos efectos que a las firmas manuscritas. Además, los Estados miembros deben garantizar la aceptación transfronteriza de las firmas electrónicas cualificadas, en el contexto de la prestación de servicios públicos y no deben introducir requisitos adicionales, que puedan crear obstáculos a la utilización de tales firmas[733].

Se trata de lograr la interoperabilidad, sin requerir una infraestructura nueva de comunicación, sino a través de los puentes ya existentes[734]. Este empeño regulatorio exclusivo por las firmas electrónicas cualificadas, a pesar de que no siempre son necesarias en la práctica, se debe a que ayudan a la gestión de la interoperabilidad y evitan el riesgo, debido a la tecnología utilizada en esta firma, que además se entiende que está estandarizada[735].

El Considerando 50 del Reglamento reconoce que los Estados miembros usan formatos de firma electrónica avanzada diferentes, para firmar electrónicamente sus documentos, por lo que considera preciso velar por que los Estados miembros puedan soportar técnicamente, al menos, una serie de formatos de firma electrónica avanzada cuando reciban documentos firmados electrónicamente.

Por consiguiente, el Artículo 27,3 dice que "los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea superior al de una firma electrónica cualificada".

Se trata promover el uso de estándares de firma electrónica, dentro de las recomendaciones realizadas por la UE, tratando de centrarse en un área de aplicación

[733] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012 (COM (2012) 238 final. Bruselas 4. 6. 2012).
[734] TAUBER, A; KUSTOR, P KARNING, B**:** "Cross border certified electronic mailing: A European perspective", *Computer&Law&Security Review*, febrero, 2013, vol. 29, núm. 1, 28 – 39.
[735] SEALED, DLA PIPER AND ACROSS COMMUNICATIONS: *Study on the standardisation aspects of eSignature*, Bruselas, 2007.

menos compleja y, por tanto, más accesible. Estas recomendaciones fueron las de promover: la interoperabilidad entre Estados miembros de la UE, el reconocimiento legal de la aplicación de la firma electrónica simple de acuerdo con la Directiva, y un desarrollo sencillo en cualquier contexto empresarial.

Unas aplicaciones accesibles son una condición, *sine qua non*, para su adopción. Las aplicaciones, que hacen uso de firmas electrónicas, deben cumplir con unos criterios de utilización estrictos, que los usuarios deberán ser capaces de usar a través de su firma electrónica sin complejidad. Lo que se ha hecho es establecer un marco regulatorio de Gobierno electrónico dentro de la Unión Europea, encuadrándose en la globalidad de acciones de promoción de la Sociedad de la Información.

Antes la Unión Europea, de acuerdo con el antiguo Tratado de la UE, no tenía competencia alguna sobre materias de Administración pública. Con el TFUE, resultante del Tratado de Lisboa, la situación ha variado; pues, otorga a la Unión Europea competencias sobre la "cooperación administrativa"; de ahí, el realizar un alineamiento claro de la Administración electrónica de los Estados miembros, como un canal, más, de provisión de servicios gubernamentales y de negocio para las empresas, no como otro servicio, más, disponible en Internet.

De este modo, por ejemplo, las empresas podrán presentar ofertas en línea para contratos públicos en cualquier lugar de la UE; podrán firmar y sellar sus ofertas, además de indicar su fecha y hora por vía electrónica, en lugar de imprimir y enviar múltiples copias en papel de las ofertas mediante servicios de mensajería. Las administraciones podrán reducir las cargas administrativas y aumentar la eficiencia, con lo que ofrecerán un mejor servicio a sus ciudadanos y ahorrarán dinero a los contribuyentes. Las personas, que deseen hacer negocios en otro país de la UE, podrán crear empresas a través de Internet y presentar informes anuales en línea, todo ello con facilidad.

Esto supondrá un paso importante, en el nuevo el afán regulatorio centrado en una única firma electrónica: la cualificada. Olvidándose del resto, solo mencionadas en las definiciones del Artículo 3. Así, trata de empujar a proveedores de servicios, Administraciones públicas, ciudadanos, etc. en la dirección que marca la tecnología

propuesta en el Reglamento, y que ya marcó la Directiva, transmitiendo el mensaje de que la seguridad está sujeta al uso de esta firma electrónica; es decir, manteniéndose la prescripción tecnológica y el abandono del resto de firma electrónicas; a las que no dota de ningún posible uso concreto.

5.4.1.1. Vigencia temporal de los certificados

Una cuestión, que puede plantearnos problemas, es la actividad de certificación realizada por el prestador de servicios, en relación con la vigencia de los certificados, respecto a los cuales, como recogen las Leyes, deben tener una duración definida, lo que a la vez supone la imposibilidad de hablar de una garantía ilimitada de seguridad.

Este problema viene a plantearse en base al principio de libre acceso, recordemos que en virtud de este principio, los prestadores de servicios de certificación europeos, no están sujetos a autorización previa en la consagración de un sistema, en el que el control de los prestadores de servicios de certificación no *es ex ante* de carácter administrativo, sino *ex post*, de carácter judicial; es decir, no se ha optado por obligar a la comprobación *ab initio* de la vigencia del certificado digital, que permitiera que una vez comprobada la vigencia del certificado y una vez confrontado el sistema con el directorio del prestador de servicios, permitiera firmar o, en caso contrario, se cerrara el sistema a cualquier posibilidad de empleo de dicho certificado digital por parte de su titular.

En nuestra opinión, si se hubiera abordado con decisión el tema, implantando un sistema automático de comprobación, *a priori*, de la vigencia de los certificados en el momento en el que se firma electrónicamente algo que el estado actual de la técnica, ya se permite, se habría, en efecto, dado un paso de gigante en la búsqueda de la tan deseada seguridad jurídica; evitando, en su gran mayoría, los problemas que pueden surgir a la hora de determinar futuras responsabilidades, por la utilización indebida de un certificado.

Sabiendo que la firma electrónica, certificados y entidades certificadoras actúan como instrumentos de seguridad del comercio electrónico, en la medida que permiten

vincular de forma segura un mensaje electrónico a una determinada persona: al titular de la clave privada correspondiente a la clave pública certificada. Obsérvese que una firma digital realizada con una clave privada únicamente identifica al emisor, si existe el correspondiente certificado que vincule de forma segura a una persona determinada con un clave pública y conecta al emisor con el mensaje exacto, pero no prueba el momento de creación o envío del mensaje[736].

El Anexo II de la Directiva viene a establecer los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos, de esta forma deberán: "a) demostrar la fiabilidad necesaria para prestar servicios de certificación; b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato; c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado; d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido; e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas; f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan; g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos; h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado; i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos; j) no almacenar ni copiar los datos de creación de firma de la

[736] MATÍNEZ NADAL, A.; FERRER, J.L.: "El problema temporal del sistema de certificados en el comercio electrónico", *Revista de la Contratación Electrónica*, enero 2001, núm. 1, págs. 1 -23.

persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves; k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado; l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que: sólo personas autorizadas puedan hacer anotaciones y modificaciones; pueda comprobarse la autenticidad de la información; los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado; y, el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados".

Pese a que entre los requisitos exigidos a los prestadores de servicios de certificación figura garantizar que pueda determinarse con precisión la fecha y la hora en la que se expidió o revocó un certificado, la Directiva[737] no exige el empleo de sellos temporales de la firma de los mensajes, de gran importancia práctica para asegurar el correcto funcionamiento del sistema de certificados[738].

La prueba del tiempo se presenta necesaria[739], en determinados casos en el ámbito del comercio electrónico, en general, y para el correcto funcionamiento del sistema de certificados en particular. Hay muchas situaciones en las que la prueba del tiempo

[737] Por el contrario, si aparecen regulados en el Reglamento 910/2014, recogiendo el sello de tiempo electrónico y el sello cualificado de tiempo electrónico. El primero lo define como los "datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante" (Artículo 3,33); el segundo como "sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42" (Artículo 3,34) Ambos serán emitidos por los servicio de confianza (cualificado en caso del segundo), el cual se encargará de su creación, verificación y validación (Artículo 3,16-a).

[738] MIGUEL ASENSIO, P.A.: "Regulación de la firma electrónica: balance y perspectiva", *Direito da Sociedade da Informaçao*, Coimbra, 2004, págs. 115 – 143.

[739] Con este sellado de tiempo se pretende establecer un método uniforme para probar qué un conjunto de datos existió antes de un momento dado y, además, qué ninguno de estos datos ha sido modificado desde entonces. Como sabemos el sellado de tiempo proporciona un valor añadido a la utilización de firma electrónica.

exacto de una determinada acción, transmisión, creación o recepción de un documento, o tiempo en que se realiza una acción o declaración de voluntad, es crucial.

Así, en caso de verificación de una firma digital, como es sabido, los certificados tienen un periodo temporal de validez, debido a la vida limitada de las claves, finalizado el cual expiran. Esta temporalidad de los certificados reconocidos implica que[740]:

a) Una vez expirada la vigencia, decae la equivalencia sentada respecto a la firma manuscrita.

b) Desaparece también la presunción de que las firmas creadas con posterioridad a ese momento, utilizando la clave pública referida en el certificado, fueran generadas por el signatario o por otra persona con su consentimiento.

c) El prestador de servicios de certificación no asumirá responsabilidad por los errores o inexactitudes, que se hubieran deslizado en el certificado, en el momento de su emisión, con respecto a los terceros que, una vez expirado su plazo de vigencia, hayan actuado confiando en él. Sin embargo, sí responderá, como es lógico, aun después de sobrepasado el plazo de vigencia, por aquellos perjuicios que se hubieren generado con anterioridad, por lo que un certificado cuyo plazo de vigencia ha terminado puede seguir siendo útil en el proceso de verificación de dichas firmas.

Ante esta situación, hemos observado diferencias en la normativa, el Reglamento italiano relativo a la formación, archivo y transmisión de documentos con instrumentos informáticos o telemáticos, establece, en su Artículo 1, h), que un certificado debe establecer su fecha de caducidad, que, en ningún caso, será superior a los tres años. El Reglamento alemán de firma digital, § 7 (1), establece que el periodo de validez de un certificado no puede exceder de 5 años (sin que entre la emisión y el inicio del periodo

[740] LAFUENTE SUÁREZ, M: "Análisis de la Ley 59/2003, de firma electrónica, tras dos años de vigencia: problemas no resueltos en torno a los certificados de firma electrónica", *Revista Aranzadi de Derecho de las Nuevas Tecnologías*, 2006 - 2, núm. 11, págs. 1 – 24.

de validez del certificado puedan transcurrir más de 6 meses). Nuestra Ley 59/2003 por mandato del Artículo 8.2, nos dice que los certificados de firma electrónica avanzada tienen una vigencia limitada a cinco años, y que en cualquier caso el resto de certificados deberán acomodar su vigencia a la seguridad que ofrezca la tecnología empleada.

Por otra parte, se presenta el problema del tratamiento de los supuestos de pérdida de vigencia[741], antes del plazo inicialmente establecido en el certificado. En la práctica, los supuestos en los que la extinción anticipada de la vigencia del certificado requiere de una actuación determinada del prestador de servicios de certificación se suelen calificar, en su conjunto, como supuestos de revocación, que podrá producirse, por consiguiente, tanto a instancias del signatario, como por iniciativa del propio prestador de servicios, cuando exista una justa causa, como puede ser la declaración de incapacidad o el fallecimiento, la existencia de inexactitudes en el certificado, o bien puede venir provocada por una resolución judicial o administrativa que ordene la adopción de tal medida.

En el Derecho alemán, desde el punto de vista técnico, los formatos de certificado prevén la inclusión de este elemento en el contenido del certificado, así el estándar X. 509 prevé el periodo de validez. Después de que el certificado expire, una vez que finalice el periodo de vida previsto, el vínculo entre la clave pública y el sujeto del certificado puede que no sea ya válido y, por tanto, no debe confiarse en el certificado. Por ello, un usuario de clave pública no debería usar un certificado expirado, a no ser que se use para confirmar de nuevo una acción anterior, que se había producido dentro del periodo de validez del certificado, como podría ser: la verificación de la firma de un documento que ya se había generado con anterioridad. Si usa el certificado, lo hará por su cuenta y riesgo. En Italia la utilización de un documento informático de una firma electrónica, basada en un certificado electrónico revocado, caducado o suspenso equivale a su falta de suscripción. En España, la Ley 59/2003 nos dice el Artículo 10,3 que "se establece expresamente que la pérdida de vigencia o suspensión de los certificados no tendrán efectos retroactivos y únicamente perjudicará a terceros, desde el

[741] LAFUENTE SUÁREZ, M: "Análisis de la Ley 59/2003, de firma electrónica, tras dos años de vigencia: problemas no resueltos en torno a los certificados de firma electrónica", *Revista Aranzadi de Derecho de las Nuevas Tecnologías*, 2006 - 2, núm. 11, págs. 1 – 24.

momento de la publicación en el Registro correspondiente"; no obstante, aunque el certificado electrónico avanzado haya perdido vigencia, la firma electrónica, basaba en el mismo, puede, perfectamente, encuadrarse en el concepto de firma electrónica simple y, por consiguiente, el documento puede considerarse igualmente signado, si bien con las reservas de seguridad que deben, necesariamente, adoptarse ante cualquier firma electrónica simple, que, como sabemos por lo ya estudiado, no siempre será considerada como válida en la transacción transfronteriza[742].

5.4.1.2. Cesión voluntaria de la firma electrónica

5.4.1.2.1. Marco legal existente: especial referencia a España

La confianza y la buena fe han sido los imperativos éticos que han regido el comercio hasta la actualidad. Así, podemos encontrar en nuestro ordenamiento claras referencias a la buena fe, como reconocimiento de protección a la confianza en una apariencia jurídica[743]; también, podemos encontrar preceptos que se refiere a la buena fe como sinónimo jurídico de honradez en el comportamiento humanos[744]; preceptos que

[742] Como se puede observar, la suspensión de certificados cualificados es una práctica operativa establecida por los prestadores de servicios de confianza en los Estados miembros, distinta de la revocación y que conlleva la pérdida temporal de la validez de un certificado. La seguridad jurídica impone que siempre se indique claramente la suspensión de un certificado. A tal fin, el Reglamento 910/2014 obliga a que los prestadores de servicios de confianza indique claramente la situación del certificado y, si está suspendido, el período preciso durante el cual ha sido suspendido. El Reglamento no impone a los prestadores de servicios de confianza ni a los Estados miembros el uso de la suspensión, pero si establece normas de transparencia cuando y donde esta práctica sea posible (Considerando 53). Esta se recoge tanto en el Artículo 28,5, para los certificados cualificados de firma electrónica, como en el Artículo 38,5, para los certificados cualificados de sello electrónico. En ambos se dice que los Estados miembros podrán fijar normas nacionales sobre la suspensión temporal de certificados cualificados de firma electrónica si: a) un certificado cualificado de firma electrónica ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión; b) el período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado. Debemos tener en cuenta que la Comisión podrá, mediante actos de ejecución, podrá establece números de referencia de normas relativas a los certificados cualificados de firma electrónica, lo que supone posibilidad de armonización en caso de posturas discrepantes entre distintos Estados.

[743] Artículos 464 del Código civil: "La posesión de los bienes muebles, adquirida de buena fe, equivale al título. Sin embargo, el que hubiese perdido una cosa mueble o hubiese sido privado de ella ilegalmente, podrá reivindicarla de quien la posea. Si el poseedor de la cosa mueble perdida o sustraída la hubiese adquirido de buena fe en venta pública, no podrá el propietario obtener la restitución sin reembolsar el precio dado por ella…"; Artículo 1164: "El pago hecho de buena fe al que estuviere en posesión del crédito, liberará al deudor".

[744] Artículos 1107: "Los daños y perjuicios de que responde el deudor de buena fe son los previstos o que se hayan podido prever al tiempo de constituirse la obligación y que sean consecuencia necesaria de su

se refieren a la buena fe, como estado jurídico de ignorancia sobre la lesión, que con la propia conducta se está generando a los derechos o facultades de otra persona en materia de posesión[745] y compraventa[746]; también, se toma en consideración en el plano hermenéutico, para la interpretación de los contratos o como criterio de conducta para el cumplimiento de las obligaciones; etc.

Con las nuevas tecnologías y el surgimiento del comercio electrónico, parte de la controversia fundamental se basa en la seguridad y/o fiabilidad y, además, en la seguridad jurídica. Todo va encaminado al establecimiento de los límites al usuario (persona jurídica o persona física), respecto de hasta donde le permite llegar el sistema; es decir, respecto de la certidumbre acerca del régimen jurídico aplicable a las relaciones comerciales entabladas por medios electrónicos, dando un reconocimiento jurídico de la contratación electrónica y el establecimiento de las consecuencias jurídicas derivadas de la utilización de medios electrónicos en la contratación.

Esta cualidad del ordenamiento es importante; pues, va a permitir a cada cual orientar su vida en el mundo jurídico, en base al conocimiento de la calificación jurídica que cada supuesto, de hecho, va a recibir, previsiblemente, del mismo. Se trata de que todo ciudadano, por referencia a las consecuencias comúnmente admitidas de los comportamientos humanos, sepa, en cada momento, la norma jurídica aplicable y tenga la seguridad de que se le aplicará. Asimismo, la seguridad jurídica tiene también otro sentido que es el de garantía de los derechos subjetivos: la conservación del derecho

---

falta de cumplimiento. En caso de dolo responderá el deudor de todos los que conocidamente se deriven de la falta de cumplimiento de la obligación"; Articulo 1688:"La sociedad responde a todo socio de las cantidades que haya desembolsado por ella y del interés correspondiente; también le responde de las obligaciones que con buena fe haya contraído para los negocios sociales y de los riesgos inseparables de su dirección".

[745] Artículo 433: "Se reputa poseedor de buena fe al que ignora que en su título o modo de adquirir exista vicio que lo invalide. Se reputa poseedor de mala fe al que se halla en el caso contrario" y Artículo 451: "El poseedor de buena fe hace suyos los frutos percibidos mientras no sea interrumpida legalmente la posesión. Se entienden percibidos los frutos naturales e industriales desde que se alzan o separan. Los frutos civiles se consideran producidos por días, y pertenecen al poseedor de buena fe en esa proporción".

[746] Artículo 1487: "Si la cosa vendida se perdiere por efecto de los vicios ocultos, conociéndolos el vendedor, sufrirá éste la pérdida, y deberá restituir el precio y abonar los gastos del contrato, con los daños y perjuicios. Si no los conocía, debe sólo restituir el precio y abonar los gastos del contrato que hubiese pagado el comprador"; Artículo 1488: "Si la cosa vendida tenía algún vicio oculto al tiempo de la venta, y se pierde después por caso fortuito o por culpa del comprador, podrá éste reclamar del vendedor el precio que pagó, con la rebaja del valor que la cosa tenía al tiempo de perderse. Si el vendedor obró de mala fe, deberá abonar al comprador los daños e intereses".

durante el tiempo en que se ostenta su titularidad. Así, la cuestión esencial es crear certidumbre jurídica respecto a las personas que formalizan los contratos[747].

Ante esta situación, la cuestión que se nos plantea es que, normalmente, los contratos se celebran por alguien que puede confiar en el cumplimiento del contrato por la otra parte; de tal manera que, entre estas persona, existe tal confianza si las partes se encuentran en una larga relación de negocios y, por tanto, no tienen dudas sobre el cumplimiento del contrato. Sin embargo, las nuevas conexiones pueden contener algunas dificultades. Aparte de problemas, tales como la capacidad y la voluntad de formalizar el contrato o, incluso, a la hora de formalizar el pago, cada parte tiene que asegurarse: de que la otra es quién es y del estatus jurídico contractual de la parte contratante, que tiene que ser entendida a la fuerza.

Dicho en otras palabras, y dejando al margen los supuestos delictivos de obtención fraudulenta de una firma electrónica, la situación que venimos a plantear es que, en muchos casos, se produce una cesión voluntaria de la firma electrónica sobre la base de la confianza en otra persona. Hablamos de supuestos en los que; por ejemplo, un Administrador de fincas le da su firma electrónica a su secretaría, para emitir una obligación de pago o para que emita una comunicación electrónica, que vincule a la entidad y a la comunidad de propietarios, que implica al Administrador y no a la secretaria; un abogado le entrega su firma electrónica a un becario, para que pida una nota simple o se comunique con el Registrador de la propiedad, en referencia a un asunto concreto; el padre que le entrega a su hijo su firma electrónica, para que realice gestiones con ella; incluso la realización de gestiones que pueden realizarse habiendo fallecido la persona que cede la firma, teniendo en cuenta que quien realiza o va a realizar la gestión no ha tenido conocimiento de que ha fallecido aquella.

Especial relevancia adquiere este último caso; pues puede resultar que una persona mayor encargue a una persona de su confianza que realice con su firma electrónica un contrato o una transacción con relevancia jurídica. El mandante fallece, sin que la persona que va realizar la gestión tenga conocimiento alguno, por lo que no hay, en principio, mala fe. Así, demostrado el fallecimiento del titular de la firma con

[747] MADRID PARRA, A.: "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, núm. 241, 2001, págs. 1189-1264.

anterioridad a la firma del contrato, que es, teóricamente, quien va a firmar el contrato, habrá que negar efectos jurídicos a la firma electrónica aplicada con posterioridad al fallecimiento de su titular; pues, se trata de la firma de un fallecido. El caso concreto se reconducirá a una cuestión de prueba: demostrar que de hecho existió o no representación; asimismo, se plantea otra cuestión que deviene de la propia comunicación y de la propia revocación, o no, efectiva del certificado de la firma electrónica, que puede provocar la incertidumbre de quien es el responsable, si el titular, la entidad certificadora o el usuario[748], lo que probablemente vendrá a resolverse con el sello temporal introducido en el propio certificado.

En cualquiera de los casos descritos, entra en escena un tercero, que viene a usar el certificado y que puede surgir de una relación contractual o en virtud de una relación de confianza existente, entre el titular del certificado y aquél. Sin embargo, el usuario no tendrá ninguna relación contractual directa con la entidad de certificación, aunque de esta dependa la seguridad del certificado de la firma electrónica[749].

En relación con las situaciones descritas, que nos podemos encontrar en la práctica en el mundo real, la garantía de la autenticidad y la identidad se da, a través del contacto personal o por la observancia de la forma escrita. Si las negociaciones del contrato tienen lugar en presencia de ambas partes, cualquiera de ellas sabe con quién está tratando o quien está al tanto del contenido de las declaraciones de intenciones e, incluso, respecto de la persona que acude a la gestión del asunto en cuestión. Asimismo, como sabemos, en nuestro Código Civil no se exige la firma para la perfección de los contratos, si bien exige el consentimiento, siendo la firma el medio más frecuente y habitual de expresar aquél. Sin embargo, en el mundo en línea, la firma electrónica puede cumplir las mismas funciones que la firma manuscrita. En consecuencia, es necesario que la Ley reconozca a la firma electrónica los mismos efectos que a la manuscrita, tal y como se ha hecho en la mayoría de las Leyes. La cuestión de la cesión voluntaria parece, en principio, haber pasado desapercibida al tratarse la firma electrónica.

---

[748] MARTINEZ NADAL, A.: "El problema temporal del sistema de certificados en el comercio electrónico", *Revista de la Contratación Electrónica*, núm. 1, 2000, págs. 21 – 39.
[749] MARTINEZ NADAL, A.: *Comentarios a la Ley 59/2003de firma electrónica*, Madrid, 2009, pág.408 y ss.

En nuestra Ley de firma electrónica, en el fomento de la confianza y seguridad, en el otorgamiento del marco jurídico necesario para establecer su uso, dentro y fuera del propio comercio electrónico, bajo el paraguas del principio de equivalencia funcional, si nos atenemos a lo que se entiende por firma electrónica, podemos decir que: se quiere declarar la autoría de un determinado documento electrónico, permitiendo a terceros tener la certidumbre de que dicho documento les llega íntegro e inalterado y que la Ley imputa al sujeto firmante las consecuencias jurídicas derivadas del mismo.

Cualquier medio técnico, que permita transmitir de forma inalterada e íntegra un documento electrónico, así como determinar la identidad de su autor, puede ser considerado como firma electrónica. Ahora bien, el legislador ha optado por conferir la presunción de que se cumplen tales funciones, cuando se utiliza el método de infraestructura de clave pública con determinados requisitos, sobre la base de un sistema de criptografía asimétrica, en el camino marcado por la propia Directiva 1999/93/CE sobre firma electrónica y ahora por el propio Reglamento 910/2014 sobre identificación electrónica. De esta forma, se trata que el firmante sea la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa (Artículo 2,3 de la Directiva, Artículos 3,8 y 3,13 del Reglamento y Artículo 6,2 de la Ley 59/2003).

La frase literal del Artículo 6,2 de nuestra Ley dice: "en nombre propio o en nombre de una persona física o jurídica a la que representa", ha sido recogida en términos similares a la Ley Modelo sobre Firma Electrónica, en el Artículo 2,d), que al definir firmante lo hace diciendo que es "la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa". De esta forma, trata de cubrir situaciones en las que el firmante actuaría en representación de otra persona. En la medida en que una persona pueda quedar obligada por una firma electrónica generada "en nombre propio" es asunto, que debe decidirse de acuerdo con la Ley que rige, según corresponda, la relación jurídica entre el firmante y la persona en cuyo nombre se genera la firma electrónica, por una parte; y por otra, la parte que confía en ella. Esa materia, así como otras pertenecientes a la operación subyacente, incluidas cuestiones de mandato y otras relativas a quién es responsable en último término del

incumplimiento por el signatario de sus obligaciones conforme al artículo 8 (si el firmante o la persona por él representada), queda fuera del ámbito de la Ley Modelo[750].

Por ello, teniendo en cuenta, como elemento de partida, que el firmante crea la firma electrónica (avanzada o reconocida) por medios, que solo él puede mantener bajo su exclusivo control y que en caso de impugnación de la propia firma resultará necesario la comprobación de la eficacia de la firma electrónica y, en especial, las obligaciones de garantizar la confidencialidad del proceso, así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. De esta forma, a tenor de lo establecido en el Artículo 22,2 de la Ley 59/2003 (en referencia a la obligación de solicitar la revocación o suspensión de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando tengan conocimiento de la existencia del certificado implícitamente), parece evidente que los únicos tipos de representación que se recogen son: la directa y la legal; no se pronuncia sobre la cesión voluntaria de la firma electrónica; es decir, lo que podríamos denominar, el mandato indirecto propiamente dicho.

Como sabemos, la firma electrónica cumple tres funciones: identificación, autenticación de la identificación y autorización/autenticación de la transacción. La cesión voluntaria de la firma electrónica la podríamos colocar en la última de ellas, que es donde se produce, en lo que podríamos denominar, función de control[751] (valor de control e incluso resultado del control) del dispositivo de firma electrónica. Mediante la cesión de la firma se está otorgando un mandato indirecto o una representación, como resultado de una acción unidireccional o pluridireccional, según el caso, pudiendo resultar, en la práctica, imposible deducir el valor de dicho mandato o representación.

Al hablar de mandato o representación debemos tener claro las diferencias existentes entre ambas figuras jurídicas, dado que la representación no tiene regulación independiente, instaurándose dentro de la regulación del mandato. Nuestro Código civil en el Artículo 1709 nos dice que "por el contrato de mandato se obliga una persona a

[750] CNUDMI/UNCITRAL: *Guía para la incorporación de la Ley Modelo de la CNUDMI*, Nueva York, 2002, párr.100 y ss.
[751] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.28.

prestar algún servicio o hacer alguna cosa, por cuenta o encargo de otra". El mandato puede ser expreso o tácito, el expreso puede darse por instrumento público o privado y de palabra, su aceptación puede ser también expresa o tácita, deducida esta última de los actos del mandatario (Artículo 1710 Cc.). Lo característico del mandato es la realización de actos de gestión, consistentes en el desarrollo de actos jurídicos por cuenta del mandante; así, podemos decir que el mandatario gestiona los asuntos del mandante, sin que en ningún momento "el mandatario no puede traspasar los límites del mandato" (Artículo 1714 Cc.).

Esta gestión de asuntos del mandante nos lleva a la representación. La representación es la legitimación o autorización a un sujeto, para que actúe con eficacia jurídica vinculante, para el representado frente a terceros; el mandato es el encargo que un sujeto da a otro, que lo acepta, para la gestión de los asuntos del primero. Normalmente, el mandatario está investido del poder de representación del mandante, que puede ser directa o indirecta, en la medida en que admite que la representación indirecta genera una auténtica representación[752]; pues, como indica el Prof. Díez-Picazo[753], la representación indirecta es verdadera representación, porque puede producir efectos directos entre el *dominus* y el tercero, sin necesidad de un contrato posterior traslativo de los mismos. Así, en el caso del 1717 CC, cuando se trata de cosas propias del mandante, dice el Prof. De Castro que si las partes lo sabían, no sería necesaria regulación específica, porque, en efecto, sería un caso de representación directa, y lo mismo en el caso del 287 del Código de Comercio en donde las partes no pueden saber que el representante es tal, porque sino, ex Artículo 285 del Código de Comercio, no tendría responsabilidad alguna. Por ello, ambos preceptos encuentran su sentido en el caso de que el tercero ignorase la existencia de un *dominus*, en el momento de la perfección, pero viniese en conocimiento de este hecho *a posteriori* y, para este caso, no puede hablarse de acción de enriquecimiento, porque el Artículo 287 del Código de Comercio es claro al hablar de la posibilidad de ejercitar "su acción" contra

[752] CAPILLA RONCERO, F.: "Contratos de servicios (II): Mandato y deposito" en *Derecho Civil. Obligaciones y Contratos* (Coord. Valpuesta Fernández, Mª R.), Valencia, 1998, págs. 767 y ss.
[753] DÍEZ PICAZO, L.; GULLÓN, A.: *Sistema de Derecho Civil (Volumen I)*, Madrid, 2001, págs. 569 y ss.

el mandatario o el principal, acción que necesariamente ha de ser la misma; pues, el Artículo no distingue[754].

Por otro lado, el poder de representación puede tener su fuente causal en otras relaciones jurídicas diferentes del mandato (por ejemplo, sociedad, contrato de servicios o de obras, relación laboral, etc.). El mandato agota sus efectos en la relación directa o indirecta entre mandante y mandatario, sin perjuicio de los efectos que produzca a terceros, cuando se obra al amparo de un poder legal de representación, que tenga por base la relación de mandato, pudiendo haber, en consecuencia, un mandato representativo y un mandato no representativo (Artículo 1717 Cc), así como puede haber representación que no obedezca a relación de mandato. Cuestión distinta es que en nuestro ordenamiento jurídico resulte imposible construir una noción abstracta del poder de representación y que, en la mayor parte de las ocasiones, la relación jurídica subyacente a la representación sea precisa el mandato. De ahí se justifica la afirmación de que la representación sea externa, en las relaciones con terceros, de la relación jurídica de mandato[755].

En el tráfico económico, la intermediación y la cooperación entre agentes económicos son frecuentes, lo que motiva la existencia de normas mercantiles que regulan las diversas figuras de mandato mercantil, éstas van desde: el contrato de comisión mercantil (Artículo 244 y siguientes del Código de comercio), mandato mercantil, en virtud del cual el comisionista se obliga a participar en un acto o contrato mercantil por cuenta de otra persona llamada comitente; se basa en la confianza, hecho por el cual, no puede cederse a un tercero[756]; el contrato de agencia, a través del cual, una persona natural o jurídica, denominada agente, se obliga frente a otra, de manera continuada o estable, a cambio de una remuneración, a promover actos u operaciones de comercio por cuenta ajena o a promoverlos y concluirlos por cuenta y en nombre ajeno, como intermediario independiente, sin asumir, salvo pacto en contrario, el riesgo y ventura de tales operaciones (Artículo 1 de la Ley 12/1992, de 27 mayo, sobre contrato

[754] FRANCH QUIRALTE, E.: "La representación en los negocios jurídicos", *Registradores y Notarios*, 9 de abril de 2003.
Disponible en: http://www.notariosyregistradores.com/ (última visita: 18/6/2014).
[755] CAPILLA RONCERO, F.: "Lección 36ª. Contratos de servicios (II): Mandato y Deposito" en *Derecho Civil. Obligaciones y Contratos* (Coord. Valpuesta Fernández, Mª R.), Valencia, págs. 767 y ss.
[756] Sentencia del Tribunal Supremo de 25 de enero de 1989.

de agencia)[757]; e incluso, la mediación o el corretaje, contrato atípico que carece de regulación general, se trata de un contrato por el cual un sujeto pone en relación con su cliente con un tercero, con el fin de concertar un contrato determinado, que de celebrarse, generaría una remuneración para el corredor[758].

5.4.1.2.2. Legitimidad de la cesión voluntaria

En adaptación al formato electrónico, cuando se hace un pedido electrónico, no se sabe si, realmente, se coloca a la persona, que se hace pasar por el comprador y, por tanto, si es éste quien realmente ordena la gestión. El contenido de una orden se puede cambiar para el receptor y viceversa. De esta forma, habría que preguntarse, ¿quién garantiza que un mensaje codificado, en realidad, se origina a partir de la persona que creó el texto con una firma con nombre o en nombre de una persona específica? Está pregunta debe formularse teniendo en cuenta que, en la cesión voluntaria de la firma electrónica puede que lo que se esté produciendo sea un fenómeno de "fungibilidad" en lugar de representación[759].

La respuesta parece lógica; pues, a tenor de la Ley, el prestador de servicios de certificación es la persona física o jurídica, que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica (Artículo 2,2 de la Ley 59/2003; Artículo 2,11 de la Directiva 1999/93/CE; Artículo 3,14 del Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior).

No obstante, nos encontramos que prestadores de servicios de certificación como, por ejemplo, la Fábrica Nacional de Moneda y Timbre (FNMT), en la actualidad, no expide certificados de representación de persona física, aun cuando la persona que actúe por representación pueda acreditar que es el representante legal o voluntario del representado; pues esta opción, que en principio puede parecer válida, se ha descartado por el riesgo legal, que se pueda hacer de dicha representación, en cuanto al uso no

[757] ESPAÑA: Sentencia de la Audiencia Provincial de Barcelona de 21 de junio de 2011.
[758] ESPAÑA: Sentencia del Tribunal Supremo de 27 junio de 2011.
[759] MADRID PARRA, A.: "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, núm. 241, 2001, págs. 1189-1264.

autorizado o fraudulento del certificado (si el representado ha fallecido, revocación del poder o la sentencia no adquirió firmeza)[760]; dicho en otras palabras, si por la índole de la relación jurídico-económica de que se trate, o de otra naturaleza, hubiese que asegurar que los efectos jurídicos le serán siempre imputados al titular del certificado[761] y que es éste quién realiza la orden, haciendo uso efectivo de la firma electrónica y no otra persona; puede que sea difícil garantizar la representación, en el sistema actual, a no ser que el último paso del proceso de aplicación del dispositivo de creación de la firma requiera la comprobación de un elemento físico irreemplazable del titular de la firma. En este caso la firma electrónica estaría funcionando, aún con mayor propiedad, como un DNI electrónico[762].

De esta forma, el sistema de representación creado, en la Ley de firma electrónica, se ha limitado al juego de la representación directa y legal; esto es, aquellas en las que, además, de los requisitos de legitimación, para actuar en la esfera ajena, un negocio jurídico representativo, sustitución del representado y consentimiento de éste vía poder o ratificación, exige una *contemplatio domini*; es decir, la actuación en nombre ajeno. De la propia literalidad del término, se deduce su sentido, que es en la que las partes conocen la existencia de un *dominus* detrás de la actuación del representante[763].

El sistema creado, en nuestra opinión tiene debilidades. Podría considerarse, para este caso concreto, que los estándares de seguridad son demasiado altos, todo está en manos de la tecnología y ésta, por sí sola, no establece la confianza que necesitan los usuarios; pues, en este sentido se está creando un vacío de representación, que se viene dando en la práctica habitual. Esto nos lleva plantearnos: hasta qué punto la cesión voluntaria de la firma electrónica e, incluso, la representación de persona física, a través de la firma electrónica, puede establecer confianza, especialmente, en los casos en los que un certificado emitido por un prestador de servicios de certificación podría limitar el riesgo de la responsabilidad, mediante la simple elección de la forma jurídica

[760] Fábrica Nacional de Moneda y Timbre (FNMT).
Disponible en: https://www.sede.fnmt.gob.es/certificados/persona-fisica (última visita: 26/6/2014).
[761] No obstante, el Artículo 3,14 del Reglamento define el "certificado de firma electrónica, una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona" abre una vía a la representación.
[762] MADRID PARRA, A.: "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, núm. 241, 2001, págs. 1189-1264.
[763] MONTES PENADES, V.L.: "La representación" en *Derecho Civil. Parte general* (Coord. López, A.; Montes, V.L.), Valencia, 1998, págs. 571 y ss.

adecuada, cualquiera que sea la figura jurídica recogida en nuestro Código civil, partiendo del principio de equivalencia funcional.

De esta manera, se daría más certidumbre jurídica a la estructuración de un sistema de certificación o acreditación de los dispositivos, que generan las firmas electrónicas y de los proveedores de servicios de certificación y, a la vez, se establecerían determinadas presunciones legales, que facilitarían la operatividad real de la firma electrónica, sin la cual difícilmente podría cumplirse esta función práctica, que viene desarrollándose, en el día a día, entre los propios usuarios de la firma.

El hecho anterior debería llevar a preguntarnos: ¿De qué manera puede el firmante transferir el control exclusivo a otras personas, si así lo desea? o ¿El control exclusivo es un hecho evidente para el firmante o es, simplemente, un hecho técnico que se puede comprobar por un tercero? La respuesta viene dada por la propia estructura triangular, reflejo, no ya de una específica ciencia o tecnología, sino incluso de un concreto modelo de aplicación: la infraestructura de clave pública.

Observando la cadena producida en la infraestructura de clave pública, para imputar un determinado documento electrónico al sujeto, que trata de identificarse y vincularse con aquél, vemos que: el firmante tiene que confiar, necesariamente, en el sistema del proveedor de servicios de certificación; que el proveedor de servicios confía en la certificación y auditoría de los organismos que lo supervisan, dentro del sistema (también lo hace el firmante indirectamente); y que el firmante no tiene que confiar en terceros, basta con que confíe en el prestador de servicios. Por otro lado, vemos que el firmante puede ceder la posibilidad de la creación de firmas a una tercera persona sin esfuerzo alguno; la transferencia del control exclusivo podría ser detectable si se estructuraran los medios; y que la transferencia del control es lo único que no se puede transmitir[764].

Si bien, tanto la Directiva como la Ley, lo que pretenden es la capacidad de mantener las claves criptográficas privadas bajo el control exclusivo de uno, cualquiera

[764] KUTYŁOWSK, M.; BŁASKIEWICZ, P.; KRZYWIECK, L.; KUBIAK, P.; PALUSZYNSKI, W.; TABOR, M.: "Technical and Legal Meaning of "Sole Control" – Towards Verifiability in Signing Systems", *Wrocław University of Technology, Trusted Information Consulting, Warsaw*, 2011. Disponible en: M.:kutylowski.im.pwr.wroc.pl/articles/lit2011-talk.pdf (última visita: 19/6/2014).

de los signatarios pueden decidir renunciar a este control y permitir a otros a firmar en su nombre, de forma voluntaria. Podría decirse que si un signatario entregó el control exclusivo de su clave privada, ya no habría un "vínculo único" entre la firma y el firmante. Este argumento es erróneo, ya que todavía existe el enlace único al signatario original, a pesar de que no firmó el documento, la firma todavía permite identificarlo[765]. De esta forma, nos situaríamos en el ámbito de la representación indirecta, considerada como verdadera representación. Por ello, puede determinarse que en el régimen de firma electrónica, la cesión voluntaria actual se encuentre recogida, implícitamente, dentro del esquema de la firma electrónica marcado en la "definición" legal, establecida en los Artículos 3 y 6,2 de la Ley.

5.4.1.2.3. Reconocimiento internacional del certificado de representación

La representación plantea otra cuestión de fondo, su reconocimiento internacional, teniendo en cuenta el carácter, necesariamente, internacional del comercio electrónico. La posibilidad de encargar a otra persona la gestión de un asunto o negocio reposa sobre la base de la autonomía de la voluntad, sin que la insuficiencia de los tipos legales sea causa de exclusión de este tipo de actuación. La Ley determina los medios legales para la atribución de la representación voluntaria a otra persona, mediante el apoderamiento, mandato, la comisión mercantil, etc. figuras sometidas a una regulación específica, que no pueden dejarse sin efecto. Así pues, la configuración de una figura como la representación voluntaria, en general, así como de la representación indirecta, no puede ser nunca contraria al ordenamiento, puesto que la base de dicho negocio no es extraña al mismo.

Teniendo en cuenta que el Reglamento 593/2008, de 17 de junio de 2008, sobre la Ley aplicable a las obligaciones contractuales (Roma I)[766] no resulta aplicable "la

[765] SORGE, C.: "La clasificación legal de las firmas basadas en la identidad", *Computer Law & Security*, abril 2014, vol. 30, núm. 2, págs.126-136.

[766] Reglamento 593/2008, del Parlamento Europeo y del Consejo, de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Roma I).
Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/jl0006_es.htm (última visita: 26/6/2014).

posibilidad para un intermediario de obligar frente a terceros a la persona por cuya cuenta pretende actuar, o para un órgano de obligar a una sociedad, asociación o persona jurídica" (Artículo 1,g). Se entiende aplicable el Artículo 10,11 del Código civil que nos dice que "a la representación legal se aplicará la ley reguladora de la relación jurídica de la que nacen las facultades del representante, y a la voluntaria, de no mediar sometimiento expreso, la Ley del país en donde se ejerciten las facultades conferidas", siendo en este ámbito donde cobra toda su relevancia.

Este Artículo viene a establecer una norma de protección del tráfico jurídico para la representación voluntaria según la cual, la eficacia directa o indirecta de la representación no se someterá necesariamente ni a la ley rectora del contrato de mandato o comisión, ni a la ley rectora del contrato concluido con el tercero, sino a la Ley del país donde el intermediario ejercita las facultades conferidas, salvo que medie sometimiento expreso a otra ley[767].

La cuestión se resolverá, respecto de las reglas que contiene el Artículo 11 del Código civil, en relación con la forma de los actos y contratos, porque este Artículo resuelve únicamente cuestiones en torno a la validez de distintas formas, en el ámbito del Derecho Internacional Privado, en armonía con el principio general de libertad de forma, para los contratos en nuestro Derecho interno (Artículos 1.278 y siguientes del Código Civil); o respecto de las reglas del Artículo 12 donde se trata de precisar la aptitud de un documento extranjero para acceder, por ejemplo, al Registro español[768].

La eficacia en España, respecto del juicio sobre las facultades representativas de poderes otorgados en el extranjero, a fin de otorgar validez a la representación voluntaria, habrá que estar, primero a la voluntad de las partes y, en su defecto, a la del lugar de ejercicio; es decir, "Ley del país en donde se ejerciten las facultades conferidas". Esto supone que para utilizar un poder extranjero, en España, es necesario adaptarse a la ley española, que en virtud del Artículo 1280 exige documento público.

[767] GARCIMARTÍN ALFÉREZ, F. J.: "Comentario al Artículo 10,11", en *Comentarios al Código civil (Tomo I)* (Dir. BERCOVITZ RODRIGUEZZ CANO, R.), Valencia, 2013, pág. 326.

[768] Resolución de 11 de junio de 1999, de la Dirección General de los Registros y del Notariado, en el recurso gubernativo interpuesto por el Notario de Torroella de Montgrí, don Leopoldo de Urquía y Gómez contra la negativa de la Registradora de la Propiedad de Bisbal d'Empordá, doña Raquel Laguillo Menéndez-Tolosa, a inscribir una escritura de compraventa, en virtud de apelación del recurrente (BOE núm. 166, Martes 13 julio 1999.
Disponible en http://www.boe.es/boe/dias/1999/07/13/pdfs/A26415-26417.pdf (última visita: 25/6/2014).

No obstante, atendiendo al tenor literal del Artículo 11 ("Las formas y solemnidades de los contratos, testamentos y demás actos jurídicos se regirán por la ley del país en que se otorguen") parece deducirse que en materia de forma debe reputarse adecuado que un documento privado sea válido siempre que esté debidamente legalizado, así lo reconoce nuestro Tribunal Supremo en Sentencia de 1 de marzo de 1993 que dice que "el Artículo 11,1 reconoce la misma validez a los contratos no acomodados a la forma y solemnidades del lugar donde se otorguen, si cumplen las formalidades exigidas por el Derecho español"[769].

La legalización ha sido tratada por la Dirección General del Registro del Notariado, que en Resolución de 11 de junio de 1999, viene a decir, conforme a la doctrina de "la equivalencia de forma", que el poder extranjero debe reunir unas formas, si no idénticas, al menos, equivalentes a las españolas y siempre que no infrinjan el orden público español. Por ello, debe reunir, como mínimo, unos requisitos: estar autorizados por Notario o empleado público competente; o sea, el autorizante ha de ser el funcionario titular de la función pública de dar fe, bien en la esfera extrajudicial o judicial; que se hayan observado las solemnidades requeridas por la Ley, lo que se traduce en el cumplimiento de las formalidades exigidas, para cada categoría de documento público; que el poderdante asuma el contenido del poder; y, por último, que el documento contenga la Apostilla de la Haya o la legalización diplomática según el país de procedencia[770]. Lo que nos lleva a lo comentado respecto a la Apostilla electrónica, tratada en el capítulo III[771].

5.4.1.3. Factura electrónica

Cuando hablamos de factura electrónica decimos que es una denominación genérica, que se refiere al uso de ficheros electrónicos como soporte de las facturas emitidas a clientes. El factor fundamental de la factura telemática es el reconocimiento

[769] MARTORELL ZULUETA, P. (Coord.): *Código civil: jurisprudencia sistematizada*, Valencia, 2011, págs. 275.
[770] MONDARAY PEREZ, F.: "La comparecencia en nombre ajeno", en *Derecho notarial* (Coord. BORRELL, J.), Valencia, 2011, págs. 217 y ss.
[771] Véase, el Capítulo tercero, en referencia a la Conferencia de la Haya: las e-Apostilla (págs. 110 y ss.).

que tiene, o que debe tener, por parte de las distintas agencias estatales de administración tributaria de los soportes electrónicos, gracias al uso de la firma electrónica[772].

La facturación electrónica es un equivalente funcional de la factura en papel[773], que consiste en la transmisión de facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos[774].

La factura tradicional es un medio de prueba importante y muy empleado en los asuntos de ámbito fiscal, mercantil o civil. Dicho valor probatorio se traslada a la factura electrónica, emitida de conformidad con las diversas disposiciones que la regulan, por aplicación del principio de equivalencia funcional y con las normas en materia de firma electrónica[775]. Esto hace que se constituya un campo obligado de tratar; pues, el uso de las facturas electrónicas puede facilitar el comercio internacional.

La factura electrónica es enviada del vendedor o proveedor del bien o del servicio al comprador o cliente, mediante un medio de comunicación específico, que registra y documenta la venta o la provisión del bien o servicios referidos[776]. No obstante, la facturación está sometida a determinados requisitos legales por las autoridades fiscales y tributarias de cada país, de forma que no siempre es posible remitir electrónicamente las facturas a la contraparte.

Hemos de observar que la factura electrónica tiene varios puntos de vista diferentes: el punto de vista de la empresa emisora, que tendrá, entre otras muchas obligaciones, firmar electrónicamente la factura, así como contar con la aceptación por

[772] WÉRY, É.: *Facturer électroniquement: droits européen, français et belge*, 2007, Bruselas, págs. 15 y ss.
[773] Como hemos comentado, el Anteproyecto de Ley de Código Mercantil regula la factura electrónica. Lo hace en su Artículo 421,9 diciendo que "la factura emitida mediante comunicación electrónica equivale funcionalmente a la factura emitida en soporte papel, produciendo idénticos efectos siempre que reúna los requisitos que le son legalmente exigibles, mantenga la integridad de su contenido y pueda ser atribuida indubitadamente a su emisor". (Véase, Capítulo primero, en referencia a España, pág. 54).
[774] RODRIGUEZ LÓPEZ, A.: "Aspectos normativos de la factura electrónica o e-factura en el ámbito europeo", *Revista de la Contratación Electrónica*, año, 2012, núm. 117, págs. 67 – 76.
[775] ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 198 y ss.
[776] RODRIGUEZ LÓPEZ, A.: "Aspectos normativos de la factura electrónica o e-factura en el ámbito europeo", *Revista de la Contratación Electrónica*, año, 2012, núm. 117, págs. 67 – 76.

parte del receptor, respecto al uso de esta modalidad de facturación; el punto de vista de la empresa receptora, que tendrá muchas obligaciones, pero destacaremos la de disponer de un software apropiado, que permita verificar la firma y la identidad del emisor, así como la vigencia del certificado; y por último, el punto de vista del sector público recaudador, que tendrá que declarar la validez de las facturas que han sido emitidas.

La factura electrónica está siendo impulsada por las agencias recaudadoras de impuestos de todos los países, demostrando que es un fenómeno global, impulsado como una prioridad en la agenda de un creciente número de Gobiernos, como una medida para controlar el pago de impuestos, ya que con la tecnología tienen capacidad suficiente para garantizar los ingresos fiscales correctos, mejorar la capacidad de vigilancia y supervisión reglamentaria, reducir los costos regulatorios y mejorar las opciones y oportunidades de aplicación de oficiales.

De esta forma, como venimos diciendo los Estados, especialmente, sus administraciones tributarias, no son ajenas a la factura electrónica[777]; por un lado, los países han emprendido modificaciones legales, para tratar de adaptar sus diferentes ordenamientos jurídicos a esta nueva realidad; y por otro, las administraciones tributarias han emprendido proyectos y programas específicos para promover el cumplimiento de las obligaciones fiscales, a través de esquemas que simplifiquen el acceso a la información y a los servicios tributarios, utilizando las TICs como medio y herramientas fundamentales[778].

Teniendo en cuenta la normativa existente, generalmente, la tecnología que emana, principalmente, de diversos requisitos legales y reglamentarios, podemos mostrar los obstáculos que se han creado. La peculiar situación de cada país, en materia de fraude fiscal, hace que las administraciones desarrollen procedimientos muy garantistas, complicando los mismos hasta hacerlos, en algunos casos, totalmente inviables desde el punto de vista tecnológico. Hay, prácticamente, tantas tipologías de

[777] WÉRY, É: *Facturer électroniquement: droits européen, français et belge*, 2007,Bruselas, págs.39 y ss.
[778] Organismos internacionales como la Organización para la Cooperación y Desarrollo Económicos (OCDE), el Centro Interamericano de Administraciones Tributarias (CIAT), el International Tax Dialogue (ITD) o la Intra-European Organisation of Tax Administrations (IOTA), entre otros, han impulsado entre sus países miembros y no miembros el desarrollo de proyectos y programas para impulsar mayores niveles de eficiencia y eficacia en el cumplimiento voluntario de obligaciones fiscales a través del uso apropiado de la tecnología.

facturas electrónicas como países. A su vez, en cada país, a nivel sectorial, se definen multitud de guías específicas, en ocasiones con estándares diferentes e, incluso, dentro de un mismo estándar y sector, con versiones diferentes. Tengamos presente que la factura es una transacción, de entre las muchas a intercambiar.

Existen múltiples escenarios que añaden complejidad a la factura electrónica[779]. No es lo mismo un proyecto de facturas de ventas (cuentas a cobrar) que otro de facturas de compras (cuentas a pagar). Cada proveedor y cliente, sector, país, etc. tendrá diferentes requisitos. La tecnología relacionada con las facturas electrónicas es muy variada; conviven diferentes formatos (e-factura, edifac, ubl, pdf firmado, etc.), tipos de sistemas de autenticidad e integridad (firma electrónica, EDI o intercambio electrónica de datos y la gestión efectiva de las pistas de auditoría interna), canales de comunicación (web services, AS2, Redes VAN, etc.) en la emisión y recepción de facturas e identificación y firma del emisor.

En la Unión Europa existe normativa aplicable destinada a realizar un modelo global de intercambio de facturas en todos los Estados miembros. Todo lo relativo a la factura electrónica se regula en la Directiva 115/2001/CE, de 20 de diciembre, por la que se modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el Impuesto sobre el Valor Añadido. Esta directiva se complementa con la posterior aprobación de la Directiva 2006/112/CE, relativa al sistema común del impuesto sobre el valor añadido, y la Directiva 2010/45/UE del consejo de 13 de julio de 2010 por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a las normas de facturación, y la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica[780], que ha sido derogada por el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[779] RODRIGUEZ LÓPEZ, A.: "Aspectos normativos de la factura electrónica o e-factura en el ámbito europeo", *Revista de la Contratación Electrónica*, año, 2012, núm. 117, págs. 67 – 76.

[780] Toda la normativa se encuentra disponible en:
- http://europa.eu/legislation_summaries/other/l31006_es.htm (última visita: 18/3/2014)
- http://ec.europa.eu/taxation_customs/vies/faq.html (última visita: 18/3/2014).

Como hemos dicho, la Directiva 115/2001 de 20 de Diciembre busca simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el Impuesto sobre el Valor Añadido. De esta forma, el Artículo 3, c), párrafo 2º establece que "las facturas transmitidas por medios electrónicos serán aceptadas por los Estados miembros a condición de que se garantice la autenticidad de su origen y la integridad de su contenido":

a) Por medio de una firma electrónica avanzada con arreglo al apartado 2 del Artículo 2 de la Directiva 1999/93/CE; sin embargo, los Estados miembros podrán exigir que la firma electrónica avanzada esté basada en un certificado reconocido y la cree un dispositivo seguro de creación de firmas, con arreglo a los apartados 6 y 10 del Artículo 2 de dicha Directiva;

b) Por medio de un intercambio electrónico de datos (EDI), tal como se define en el Artículo 2 de la Recomendación 1994/820/CE de la Comisión, cuando el acuerdo relativo a este intercambio prevea la utilización de procedimientos, que garanticen la autenticidad del origen y la integridad de los datos.

c) Por otros medios, a reserva de su aceptación por el o los Estados miembros de que se trate. De esta forma los Estados miembros tienen la opción de introducir soluciones nacionales específicas, lo que crea nuevas barreras para el uso transfronterizo de la firma electrónica avanzada. Muchos países han optado por ello, que, en la práctica, conduce a que no sea posible utilizar la firma electrónica a través de fronteras, ya que el reconocimiento mutuo no funciona en la práctica.

Las facturas EDI[781] van ligadas a un proceso de compra de mercancía, pero no se lleva bien con la facturación de servicios, donde la facturación XML es más sencilla de uso. En los servicios tampoco suele haber un proceso de pedido-albarán-factura.

[781] WÉRY, É. *Facturer électroniquement: droits européen, français et belge*, 2007, Bruselas, págs. 83 y ss.

En nuestra opinión, el problema principal de EDI es que al ser un sistema propietario, que lo hace costoso. Sólo lo utilizan los que por su relación, con grandes empresas de distribución, están forzados a ello, ya que contempla en su totalidad la cadena de aprovisionamiento de los clientes. Otras empresas, sin esta obligación, por lo tanto, no pueden recibir ni emitir EDI.

La factura electrónica, según se contempla en la legislación europea y española persigue que sea adoptada por la universalidad del tejido empresarial. Ahora mismo, en la Comisión Europea, para la factura electrónica, se está trabajando en un esquema único para que sea adoptado por todos los Estados miembros[782]. Si EDI fuera lo mejor, quizá no se estaría invirtiendo tiempo y dinero, trabajando en diseñar otro formato.

Las facturas emitidas vía firma electrónica reconocida, es el escenario más frecuente. Los diferentes requisitos nacionales, para la firma electrónica, hacen que sea costoso y difícil, para las empresas utilizar las facturas electrónicas a nivel internacional. En la práctica, ésta es una de las razones por las que grandes empresas evitan el uso de la facturación electrónica en un determinado país[783]. Una solución podría ser la subcontratación de este servicio a una empresa, que permita convertir las facturas electrónicas y agregar el tipo de firma electrónica que se requiere por cada país, lo que incrementa el coste.

Por otra parte, la Directiva establece la reserva de aceptación por el o los Estados miembros de que se trate de la factura electrónica. Si se emite vía firma electrónica, está dando a los Estados miembros la opción de introducir soluciones nacionales específicas, lo que crea nuevas barreras para el uso transfronterizo[784]. Muchos países han optado por

[782] UN/CEFACT: *Annex to Recommendation No. 6: Aligned Invoice Layout Key for International Trade" to accommodate e-invoicing*, Genova, 16ª session, 8-10 de diciembre de 2010, págs. 4 y ss. (ECE/TRADE/C/CEFACT/2010/8/Rev. 1).
Disponible en:
http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec06/ECE_TRADE_C_CEFACT_2010_8E_r1.pdf (última visita: 19/3/2014)

[783] KOMMERSKOLLEGIUM/SWEDISH NATIONAL BOARD OF TRADE: "E-invoicing in cross-border trade", *UNCITRAL Colloquium on Electronic Commerce*, 14-16 de febrero de 2011, Neva York, pág. 6.

[784] KOMMERSKOLLEGIUM/SWEDISH NATIONAL BOARD OF TRADE: "E-invoicing in cross-border trade", *UNCITRAL Colloquium on Electronic Commerce*, 14-16 de febrero de 2011, Neva York, pág. 7.

esta opción, lo que supone, en la práctica, que no sea posible utilizar la factura electrónica; pues, ya que el reconocimiento mutuo no funciona en la práctica.

La Directiva se distancia de las recomendaciones dictadas por la UN/CEFACT[785], que nos dice, que las Leyes y reglamentos, no deberían exigir requisitos especiales a una factura electrónica, respecto a la forma en que se envía. Las autoridades fiscales y otras autoridades no deben presentar requisitos, que exijan soluciones técnicas, sino que deberían dejar que sea las empresas quien las desarrollen (Así lo han hecho, por ejemplo, Finlandia y Suecia). En la misma recomendación, también se afirma que los Gobiernos y las autoridades fiscales deben vigilar el desarrollo de la factura electrónica y coordinarlo con el de los mercados. Las adaptaciones y los cambios deben ser formulados sobre la base de la menor intervención posible y la armonización de la legislación debe estar dirigida por todos los organismos nacionales; de tal manera que, se pueda promover la lucha contra la delincuencia, en lo que respecta al fraude en el IVA.

5.4.1.3.1. Requerimiento de firma electrónica de persona jurídica

La factura electrónica, como es lógico, tiene que firmarse electrónicamente. Lo que supone plantearnos la problemática existente sobre la firma electrónica de persona jurídica.

Teniendo en cuenta que la firma electrónica reconocida es uno de los métodos aprobados, para la transmisión de las facturas electrónicas y que están disponibles bajo la Directiva del IVA, creando un problema añadido a la utilización transfronteriza de la firma electrónica.

Se ha creado por motivos evidentes, la Directiva 1999/93/CE sobre firma electrónica no recoge expresamente la firma electrónica de la persona jurídica, sino que se limita a señalar en su Artículo 2,3 que "firmante es la persona que está en posesión de

[785] Todas la Recomendaciones de la UN/CEFACT se encuentran disponibles en: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec_summary.pdf (última visita: 14/3/2014).

un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa", lo que deja abierta cualquier interpretación que se pueda hacer, al referirse única y exclusivamente a la persona en general[786].

En España, la dicción del Artículo 2,3 de la Directiva ha quedado fijada en el Artículo 6,2 de la Ley 59/2003 sobre firma electrónica, que señala: "firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica, a la que representa".

Se aducía como tesis opuesta que la definición de la Directiva era lo suficiente amplia y que, además, el propio Real Decreto Ley 14/1999 de firma electrónica en su Artículo 5,3 preveía, en el campo del cumplimiento de las obligaciones tributarias, y en concreto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o jurídica. Esta especificación que contenía esta norma y que estaba restringida para el campo tributario, puede que fuera contraria a la Directiva. No obstante, suponía un grave problema a la administración tributaria, que desde la aprobación del Real Decreto había expedido cientos de certificados y quería que la Ley 59/2003 confirmase lo ya regulado[787].

Ante la situación descrita, el legislador nacional ha incorporado, en su ordenamiento jurídico, la posibilidad de que la persona jurídica pueda ser titular de un certificado de firma electrónica o digital, así lo recoge no sólo el Artículo 7,1 de la Ley 53/2003 sobre firma electrónica que dispone: "podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos". De este modo, mediante tales certificados se vincula una firma electrónica a la persona jurídica, a la que se le reconoce la condición de firmante. En cuanto a sus efectos, el apartado cuarto de este Artículo 7 determina que "se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior".

[786] LOPEZ GALIANO PERONA, J.: "firma electrónica de la persona jurídica: una alteración del sistema clásico de representación", *Boletín del Ministerio de Justicia*, año LIX, 15 de octubre de 2005, boletín núm. 1999, págs.3887 – 3905.
[787] GARCÍA MAS, F. J.: "La firma electrónica de las personas físicas: comentario al art. 7 de la Ley 59/2003, de 19de diciembre, sobre firma electrónica", *Actualidad civil*, año 2005 – 2, págs. 643 – 653.

Desde el punto de vista jurídico-privado es bastante claro lo dictaminado por el Consejo de Estado, en su Dictamen 1589/2003, de 29 de mayo de 2003 donde nos viene a decir que "dicha regulación se aviene mal con el criterio inspirador de la norma plasmado en el Artículo 1,2, a tenor del cual las disposiciones de la Ley "no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten". En relación con los certificados electrónicos de las personas jurídicas, dicho criterio se hace patente en el apartado primero del Artículo 7, que establece que dichos certificados "no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica". Y se dice que la regulación proyectada se aviene mal con tal principio por cuanto la atribución de la condición de firmante a la persona jurídica implica imputarle directamente a ella, y no a través de su representante, la declaración de voluntad que la firma electrónica reconocida plasmada en un documento supone. En el mismo sentido, no cabe ignorar que, de conformidad con lo dispuesto en el Artículo 3, dicha firma electrónica reconocida tiene el mismo valor jurídico que la firma manuscrita, firma de la que, como es obvio, carecen las personas jurídicas. Y cabe agregar a lo anterior que no se advierten las ventajas que supondrá el certificado electrónico de las personas jurídicas y la atribución a éstas de la condición de firmantes respecto a la emisión de un certificado electrónico a favor de su representante o administrador, certificado en el que se puede dejar constancia de la propia relación de representación, en los términos ya previstos en el Artículo 11,4. En este último caso, la imputación de los efectos de la firma electrónica a la persona jurídica se haría a través de los cauces ordinarios de la teoría de la representación, sin necesidad de artificios tales como la atribución de la condición de firmante a la persona jurídica y sin forzar las categorías del Derecho Civil y Mercantil. En última instancia, la finalidad a que se alude en la exposición de motivos, consistente en integrar a estas entidades en el tráfico telemático puede conseguirse sin necesidad de considerar a la persona jurídica como firmante. Por ello, estima el Consejo de Estado que debiera reconsiderarse la conveniencia de mantener, en los actuales términos, la regulación proyectada. En este sentido, bastaría, además de otros ajustes a lo largo de la redacción del texto, con establecer de forma clara que en tales certificados es el solicitante, y no la persona jurídica, el que asume la condición de firmante, y que la traslación de los efectos de la firma a la persona jurídica se produce de conformidad con

los principios generales de la teoría de la representación"[788]. Respecto a este punto de vista, es significativo que en otros países como Alemania, Austria o Italia sólo se admite la firma de las personas físicas[789].

Así, el legislador español al establecer como firmante a la "persona que está en posesión…" incluye tanto a la persona física como jurídica. La norma general en el ordenamiento jurídico español sólo permite que la persona física, no la jurídica sea titular de firma electrónica; pues, se sigue el modelo de la firma manuscrita. Una persona jurídica no puede firmar, sino que lo hacen las personas físicas que actúan en su nombre, aunque las consecuencias jurídicas se le imputen a la persona jurídica. Sin embargo, es cierto, como comenta el Prof. Madrid Parra, que a efectos fiscales es más operativo otorgar una firma electrónica al ente o persona jurídica que tiene su correspondiente código de identificación fiscal. Por eso, para este concreto ámbito de derecho público el legislador contempla la posibilidad de que el signatario sea una persona física o jurídica[790].

De esta forma, la firma electrónica de persona jurídica debe verse, más desde un punto de vista jurídico-público; pues, la regulación se hace pensando en el Gobierno electrónico; es decir, lo que se buscaba desde un principio, en lo relativo a la gestión de tributos on-line, el uso de las tecnologías de la información y la comunicación en el marco de la modernización del Estado, que posibilita el acceso y la entrega de servicios gubernamentales, etc. Así se reconoce en el apartado tercero del Artículo 7: "Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

[788] CONSEJO DE ESTADO: "Doctrina legal", *Boletín Oficial del Estado*, Madrid, 2006, pág. 340

[789] En este sentido en Dictamen del Comité Económico y Social Europeo sobre la "Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior" [COM(2012) 238 final], se dice que "como quiera que en la actualidad no hay sistemas nacionales de identificación electrónica bien desarrollados para empresas (personas jurídicas) en ninguno de los 27 Estados miembros, el Comité recomienda que la Comisión, en el respeto de los principios de subsidiariedad y proporcionalidad, haga todo lo posible para una pronta introducción de un sistema voluntario de identificación electrónica europea para las personas jurídicas que incluya una determinada serie de parámetros para todas las empresas de la UE".

[790] MADRID PARRA, A.: "Seguridad en el comercio electrónico" en *Contratación y comercio electrónico*, (Orduña Moreno, F. (Dir.), Campuzano Laguillo, A.B.; Plaza Penadés, J. (Coords.)), Valencia, 2003, pág. 137; MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de Contratación Electrónica*, núm. 15, Abril, 2001, pág. 27*;* MADRID PARRA, A.: "Aspectos jurídicos de la identificación en el comercio electrónico", en *Derecho del Comercio Electrónico,* 2001, pág. 205.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico"[791].

Así, con la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos recoge los medios de autenticación de los ciudadanos, para poder interactuar con la administración en las ocasiones en las que se requiere identificación segura, recogidas en el Artículo 13.2:

a) Sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones, que en cada caso se determinen.

Para obtener información sobre qué es la firma electrónica, cómo puede obtenerse, quién puede proporcionarla, cómo y cuándo debe utilizarla, se aconseja que se acceda a

[791] Si observamos que en los demás países no se reconoce el certificado electrónico de persona jurídica nos crea problemas de reconocimiento, empresas consultadas nos han comentado ejemplos pongamos un ejemplo práctico (se trata de un hecho real comentado por una empresas de las empresas consultadas en la realización de este trabajo. Digamos que la empresa fabrica un producto que se vende en grandes almacenes y es una exigencia contractual la emisión de factura electrónica): en Portugal al inicio del ejercicio 2013 se tiene una inspección de Hacienda, y dado que en España podemos utilizar la factura electrónica, las facturas que la empresa filial portuguesa recibe de sociedades españolas son electrónicas con la pertinente firma digital. De esta forma, resulta que la sociedad portuguesa fue requerida por la Hacienda portuguesa para obtener las facturas en formato físico y sin firma digital para su aportación al procedimiento inspector pues en Portugal no se reconoce la firma electrónica de persona jurídica. Naturalmente, si hablamos de un grupo de empresas no hay problemas en convertirlas al formato físico sin firma, pero si no lo es, se crea un problema de envergadura con el consiguiente regreso al papel existente en algunos países.

la información que la Fábrica Nacional de Moneda y Timbre (FNMT) proporciona en su página web[792].

Por otra parte, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, distingue en su Artículo 10, relativo a la firma electrónica de los ciudadanos, entre personas físicas, personas jurídicas y entidades sin personalidad jurídica. En el caso de éstos últimos establece que las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica en todos aquellos procedimientos y actuaciones de la Administración General del Estado para los que se admitan. En caso de no admisión, la sede electrónica debe facilitar sistemas alternativos, que permitan a las personas jurídica el ejercicio de su derecho a relacionarse electrónicamente con la Administración General del Estado, aunque no siempre ocurre.

Asimismo, nos encontramos que, para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica, bien a través de:

a) Sello electrónico de Administración pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso, la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

[792] Disponible en CERES-FNMT: https://www.cert.fnmt.es/ (última visita: 14/3/2014)

Nos encontramos con el sello electrónico de la Administración Pública (Artículo 18 de la Ley 11/2007), que se utiliza para firmar actos administrativos por medio de sistemas informáticos, sin intervención directa de la persona física competente.

Los actos automatizados siguen siendo responsabilidad de un determinado órgano administrativo y deben sustentarse en un procedimiento concreto y conocido. Como ejemplo, de este tipo de actuaciones administrativas automatizadas, se pueden citar las siguientes: el registro electrónico de entrada que emite un acuse de recibo firmado, los volantes de empadronamiento obtenidos on-line, las notificaciones telemáticas, etc. Por consiguiente, se determina que el certificado de sello electrónico incluirá el número de identificación fiscal y la denominación correspondiente. La relación de sellos electrónicos utilizados por cada Administración pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos. Esta afirmación nos lleva determinar, en este sentido, que la relación de sellos electrónicos utilizados por la persona jurídica, respecto a la Administración, deberá ser compatible con el sello de está, lo que nos lleva a prestar especial atención a éste con el fin de poder evitar posibles problemas discriminatorios.

Ante esto, para ofrecer seguridad jurídica sobre la validez de la firma, surge la el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que detalla qué componentes de una firma electrónica cualificada debe evaluar la parte usuaria que efectúa la validación; además, define qué requisitos son exigibles a los proveedores de servicios de certificación cualificados para que puedan brindar un servicio de validación cualificado a las partes usuarias, que no desean o no pueden realizar por sí mismas la validación de las firmas electrónicas cualificadas, debiendo estimular a los sectores privado o público para que inviertan en tales servicios. Ambos elementos deben contribuir a que la validación de la firma electrónica cualificada resulte fácil y cómoda para todas las partes a nivel de la Unión.

De esta forma, cuando una transacción exija un sello electrónico[793] cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica. Los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido creado o expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento. Es importante para que sigan desarrollándose las transacciones electrónicas transfronterizas en el mercado interior, que los documentos electrónicos originales o las copias certificadas expedidas por los organismos competentes correspondientes en un Estado miembro, con arreglo a su Derecho nacional sean aceptadas como tales, también en otros Estados miembros.[794]

Sin embargo, adelantándose al Reglamento, el legislador español, con el objeto de impulsar el uso de la factura electrónica, crea un registro contable de facturas y regula, así, el procedimiento para su tramitación en las Administraciones públicas y las actuaciones de seguimiento por los órganos competentes. Esto se ha concretado en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público**,** que en su Artículo 5 (intitulado **"**Formato de las facturas electrónicas y su firma electrónica"), nos dice que Las facturas electrónicas que se remitan a las Administraciones Públicas deberán tener un formato estructurado y estar firmadas con firma electrónica avanzada basada en un certificado reconocido, de acuerdo con lo dispuesto en el Artículo 10.1.a) del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación; también se admitirá el sello electrónico avanzado basado en un certificado reconocido que reúna los siguientes requisitos: a) El certificado deberá identificar a la persona jurídica o entidad sin personalidad jurídica que selle la factura electrónica, a través de su denominación o razón social y su número

[793] COMISIÓN EUROPEA*: Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, (COM (2012) 238 final), nos viene a decir que el artículo 28 se refiere a los efectos jurídicos de los sellos electrónicos de las personas jurídicas. Se concede así unas presunciones legales específicas a los sellos electrónicos cualificadas que garantiza la autenticidad e integridad de los documentos electrónicos a los que están vinculados, recogiendo en el artículo 29 los requisitos de los certificados y en el artículo 31 la condición de validación y conservación de los sellos electrónicos cualificados.

[794] Véase, Capítulo cuarto, en referencia a la Unión Europea, la regulación, en el nuevo Reglamento, del sello electrónico, considerando éste como una verdadera firma electrónica de persona jurídica (págs. 240 y ss.).

de identificación fiscal; b) La solicitud del sello electrónico avanzado podrá formularse bien mediante comparecencia presencial de una persona física que acredite su representación, bien por medios electrónicos mediante el DNI electrónico y la remisión de los documentos que acrediten su poder de representación en formato papel o electrónico. Al final de este Artículo nos dice lo que se entiende por sello electrónico "es el conjunto de datos en forma electrónica, consignados o asociados con facturas electrónicas, que pueden ser utilizados por personas jurídicas y entidades sin personalidad jurídica para garantizar el origen y la integridad de su contenido", de manera distinta a la establecida en el Artículo 3,25 del Reglamento 910/2014, que considera "sello electrónico, datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos".

5.4.2. La equivalencia de certificados de terceros países

El Artículo 7 de la Directiva 1999/93/CE, es fundamental en este ámbito, que viene a tratar los aspectos internacionales de los certificados reconocidos, expedidos por los proveedores de servicios de certificación establecidos en un tercer país.

Este Artículo analiza los efectos de los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país no integrado en la Unión[795], regulando aspectos discriminatorios en relación con los certificados extranjeros; pues, deben reunir una serie de condiciones, marcados en el citado precepto, siempre que se trate de firmas digitales, basadas en una infraestructura de clave pública. Lo que redunda en favor de los certificados digitales emitidos por los proveedores de servicios de certificación establecidos en el territorio de los Estados miembros de la Unión Europea.

[795] ÁLVAREZ CIENFUEGOS SUAREZ, M. Jª: *La firma electrónica y el comercio electrónico en España. Comentarios a la legislación vigente*, Madrid, 2000. Pág. 79.

Así pues, un proveedor de servicios de certificación de un tercer país tiene tres opciones para conseguir el reconocimiento de sus certificados en la Unión europea[796]:

a) Cumplir los requisitos fijados en la Directiva de la Unión Europea sobre la firma electrónica y obtener acreditación en el marco de un sistema instaurado en un Estado miembro.

b) Concertar una certificación cruzada, con un proveedor de servicios de certificación establecido en un Estado miembro de la Unión Europea.

c) Operar al amparo de un reconocimiento general, otorgado a nivel de un acuerdo internacional[797].

El mencionado Artículo en el apartado a), otorga a los Estado miembros la obligación de velar por los "certificados expedidos al público por un prestador de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple algunas condiciones".

Estas condiciones son las de garantizar que cumplen con la normativa europea; o sea, con los requisitos tecnológicos y de seguridad. Además, hay que sumar los criterios que haya teniendo en cuenta cada Estado, ya que puede que hayan fijado su propio sistema de supervisión.

En definitiva, se establece la discriminación de los certificados extranjeros, al exigir a los prestadores de servicios de certificación extranjeros un mayor esfuerzo para poder actuar dentro de la Unión Europea; de tal forma que, se les obliga a que cumplan

[796] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 77.

[797] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, (COM (2012) 238 final), al hacer referencia al artículo 10 de la Propuesta describe el mecanismo para el reconocimiento y aceptación de los servicios de confianza cualificados prestados por un proveedor establecido en un tercer país. Se basa en el artículo 7 de la Directiva 1999/93/CE, pero solo conserva la única opción viable en la práctica, a saber, permitir dicho reconocimiento en virtud de un acuerdo internacional entre la Unión Europea y terceros países u organizaciones internacionales.

con el régimen jurídico establecido por el Estado[798] en el que se encuentren establecidos, más el de la Unión Europea y, en algún caso, que concretaremos más adelante, el de los Estados miembros.

Volviendo a la literalidad del precepto, con el fin de garantizar su validez jurídica, esto es, "contribuir al uso y al reconocimiento legal de la firma electrónica en la Comunidad"[799], la Directiva parece seguir la pauta marcada por el Artículo 12,5 de la Ley Modelo sobre Firma Electrónica, en la medida que parece respetar la autonomía de la voluntad de las partes, para concertar de común acuerdo, las condiciones en que aceptarán las firmas electrónicas.

Sin embargo, se aprecia un grado de discriminación notorio; porque, como se observa, la Directiva impone fuertes controles a los prestadores de servicios de certificación y solo a los que emiten una clase de certificado, a la vez que abre a los Estados miembros la posibilidad de que aumenten los criterios de responsabilidad establecidos, como mínimos, en la propia Directiva.

Por otro lado, al hablar "de acuerdos bilaterales o multilaterales entre la Comunidad y terceros países u organizaciones internacionales"[800], está condicionando el desarrollo del comercio electrónico internacional a acuerdos con terceros países en materia de reconocimiento mutuo de servicios de certificación, para garantizar la interoperabilidad a nivel mundial.

---

[798] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior,* Bruselas, 4 de junio de 2012, (COM (2012), en referencia al Artículo 5 (Artículo 6 del Reglamento) nos dice que: en el reconocimiento y aceptación mutuos de los medios de identificación electrónica incluidos en un régimen notificado a la Comisión en las condiciones establecidas en el Reglamento. La mayoría de los Estados miembros de la UE han introducido algún tipo de régimen de identificación electrónica y que estos sistemas eran diferentes en multitud de aspectos.
Por otro lado, en Artículo 20 (Artículo 27 del Reglamento) contiene las normas relativas a los efectos jurídicos de la firma electrónica de persona física reconoce: que los Estados no garantizaban la aceptación transfronteriza de las firmas electrónicas reconocidas y que, en algunos casos introducen requisitos adicionales que creaban obstáculos a reconocimiento de las firmas electrónicas.

[799] Considerando 17 de la Directiva 1999/93/CE, del Parlamento y del Consejo, de 13 de Diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

[800] Artículo 7,1-c) Directiva 1999/93/CE.

Será la Comisión quien presentará las propuestas[801]. Así, se fijan las condiciones bajo las que tiene lugar el reconocimiento recíproco de la eficacia de los certificados. Pese a la eficacia potencial, que presentan los Convenios internacionales de este tipo, se trata de una posibilidad apenas desarrollada en la actualidad[802].

De esta manera, si bien este Artículo 7 puede que tienda a valorar la equivalencia y reconocimiento de los certificados extranjeros con voluntad expansiva buscando favorecer el comercio intracomunitario; además de dar seguridad a las transacciones electrónicas procedentes de terceros países[803]. En realidad es obvio que ha tenido un efecto totalmente contrario, ya que la Directiva, en este precepto, limita toda posibilidad de reconocimiento; lo que establece son supuestos en los que los Estados miembros deben reconocer certificados emitidos por un proveedor de servicios de certificación establecido en un tercer país.

Se pone de manifiesto el hecho arriba señalado, cuando la Comisión, tras un análisis jurídico y técnico del uso práctico de la firma electrónica, evidencia que existen problemas de interoperabilidad, que limitan su uso transfronterizo, insistiendo en la necesidad de un enfoque más eficaz en materia de reconocimiento mutuo[804].

De esta suerte, pese a las disposiciones legales existentes y a los compromisos adquiridos por los Estados miembros y la Comisión, resulta necesario un enfoque más coordinado y global, para facilitar el uso transfronterizo de la identificación y la firma electrónica en la práctica, para evitar la fragmentación del mercado único, para lo cual ya propuso un "Plan de acción para promover la firma y la autenticación electrónicas"[805].

---

[801] Artículo 7,3 Directiva 1999/93/CE.

[802] MIGUEL ASENSIO, P.A.: *Derecho Privado de Internet*, Madrid, 2002, pág.419.

[803] ÁLVAREZ CIENFUEGOS SUAREZ, M. Jª.: *La firma electrónica y el comercio electrónico en España. Comentarios a la legislación vigente*, Madrid, 2000. Pág. 79.

[804] COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO EUROPEO, AL COMITÉ ECONÓMICO EUROPEO Y AL COMITÉ DE LAS REGIONES: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único*, 28 de Noviembre de 2008, pág. 5.
Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0798:ES:NOT (última visita: 14/3/2014).

[805] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: *Un mercado único para la Europa del siglo XXI*, 20 de Noviembre de 2007. Pág. 16.

Con la aprobación del Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, en su Artículo 14, hace referencia a los "Aspectos Internacionales" relativos al reconocimiento jurídico de los certificados reconocidos por del proveedor de servicios de confianza establecido en un tercer país y su equivalencia jurídica a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión.

Este Artículo se basa en lo establecido en el Artículo 7 de la Directiva, pero sólo conserva la única opción viable en la práctica para la Comisión: permitir dicho reconocimiento en virtud de un acuerdo internacional entre la Unión Europea y terceros países u organizaciones internacionales[806], de acuerdo con el Artículo 218 del TFUE.

Con la entrada en vigor del Tratado de Lisboa, la Unión Europea adquirió personalidad jurídica. En consecuencia, pasó a ser un sujeto del Derecho internacional que puede negociar y celebrar acuerdos internacionales en su propio nombre.

Estos acuerdos internacionales tienen repercusiones jurídicas en el Derecho interno de la UE y de los Estados miembros. Además, la UE puede celebrar acuerdos internacionales, en función de una serie de modalidades definidas en los Tratados Constitutivos de la UE.

El procedimiento de aprobación de los acuerdos internacionales, celebrados entre la Unión Europea y un país u organización internacional, se especifica en el Artículo 218 del Tratado de Funcionamiento de la UE, que se desarrolla en varias fases: el Consejo adopta las recomendaciones, que definen el mandato de la negociación de la Comisión; a continuación, la Comisión negocia el acuerdo y lo firma con el Consejo; siempre se consulta al Parlamento, que debe dar su aprobación en determinados casos;

Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0724:FIN:es:PDF (última visita: 14/3/2014).

[806] COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, (COM (2012) 238 final).

y, por último el Consejo celebra el acuerdo. Eventualmente, el Tribunal de Justicia puede intervenir para controlar su validez.

En principio, la decisión sobre la celebración del acuerdo se adopta por mayoría cualificada del Consejo. No obstante, el Consejo debe aprobar por unanimidad los acuerdos de asociación entre la UE y países terceros; y acuerdos relativos a ámbitos sometidos a la unanimidad.

Es cierto que la negociación y firma de tratados internacionales es la solución lógica por la reciprocidad de los efectos que pudieran producir los certificados expedidos. No obstante, en nuestra opinión, de una forma implícita, se está reconociendo la rigidez y el alto nivel de exigencia a los proveedores de servicios de confianza, a la vez que se está cerrando el mercado europeo a empresas extranjeras.

De esta manera, sí con la Directiva se reconocía, en general, la discriminación de los certificados extranjeros que reunían las condiciones que se establecían, ahora se está denegando con mayor rigidez el reconocimiento legal de las firmas y certificados extranjeros.

Dada la importancia del el carácter transfronterizo del comercio electrónico y del carácter internacional del uso efectuado de firmas y certificados electrónicos, se debería reflexionar sobre este precepto, porque si se trata de ofrecer soluciones prácticas a las cuestiones que se plantean en la celebración de contratos internacionales, se debería haber tratado el reconocimiento de certificados extranjeros, observando el principio de equivalencia sustancial del nivel de fiabilidad de los certificados extranjeros y nacionales, atendiendo al nivel de los distintos tipos de certificados existentes en línea, conforme a lo recogido en la Ley Modelo sobre Firma Electrónica.

No obstante, con la Directiva, aún en vigor, y por la forma en que regula los aspectos internacionales, se colige que uno de sus objetivos era asegurar a los proveedores de servicios de certificación de la Unión Europea condiciones de acceso a los mercados extranjeros. Al acumular el requisito de equivalencia sustancial a las normas de la Unión Europea, más el requisito adicional de “acreditación en el marco de

un sistema establecido en un Estado miembro", la Directiva exige, de hecho, que los proveedores de servicios de certificación extranjeros cumplan el régimen propio de partida, más el de la Unión Europea, lo cual es un nivel más elevado que el exigido a los proveedores de servicios de certificación acreditados en un Estado miembro de la Unión Europea. Mientras que el Reglamento establece el reconocimiento reciproco en virtud de un acuerdo internacional celebrado y, posteriormente, se garantizará que los prestadores cualificados de servicios de confianza de terceros países y los servicios de confianza cualificados que prestan, presenta un grado de fiabilidad sustancialmente equivalente[807], en relación con los requisitos aplicables dentro de la Unión Europea y viceversa; estos es, que los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios en terceros países u organizaciones internacionales.

5.4.2.1. Perspectiva estatal del reconocimiento de certificados extranjeros

El Artículo 7 de la Directiva se ha aplicado de forma diferente en los Estados miembros. En el caso de Alemania (Artículo 23 SigG) prevé el reconocimiento de firmas electrónicas extranjeras y productos para la firma electrónicas. En este Artículo se distingue entre firmas electrónicas originarias de países de la Unión Europea, los Estados de la Asociación Europea de Libre Comercio (AELC) y las firmas electrónicas originarias de terceros países.

Por un lado, establece que las firmas electrónicas basadas en un certificado reconocido de un Estado miembro de la UE o de la AELC se reconocen como jurídicamente equivalentes a las firmas electrónicas cualificadas, en el sentido de la Ley alemana, siempre que dichos certificados reconocidos cumplan con las disposiciones del Artículo 5,1 de la Directiva de firma electrónica. En consecuencia, si una firma electrónica originaria de un Estado miembro de la UE o de la AELC o de un tercer país

[807] En nuestra opinión, cuando en el Artículo 14,2 se dice que "los acuerdos a que se refiere el apartado 1 garantizarán", se pretende adoptar la regla de reciprocidad lógica, adoptando un criterio flexible de "grado de fiabilidad sustancialmente equivalente", establecido en el Artículo 12,4 de la Ley Modelo sobre Firma Electrónica.

se reconoce, como jurídicamente equivalente a las firmas electrónicas, tal y como se establece en la Ley, puede cumplir con los requisitos de la firma manuscrita y el titular puede basarse en las presunción prevista en el Artículo 292, a de la ZPO.

Por otro, en referencia a las firmas originarias de un tercer país, la Ley adopta las disposiciones del Artículo 7 de la Directiva y, además, se requiere que el certificado se utilice en el ámbito previsto por el Artículo 5,1 de la Directiva; por consiguiente, si la firma electrónica originaria de un tercer país no se reconoce como jurídicamente equivalente, conforme a los criterios establecidos para la firma electrónica cualificada, conforme al Artículo 126 BGB, el titular de la firma deberá demostrar su validez (Artículo 292, a ZPO)[808].

En Italia, el Artículo 21, párrafo 4º de la su Ley, establece que las disposiciones, relativas a los efectos jurídicos de los documentos electrónicos y firmas electrónicas, se aplicarán solo a los documentos y firmas electrónicas basadas en un certificado reconocido, emitido por los proveedores de servicios de certificación con oficinas en un país que no sea miembro de la UE, siempre que, el proveedor de servicios reúna todos los requisitos de confiabilidad prevista por la Directiva y la legislación nacional, el certificado reconocido sea otorgado por un proveedor de servicios establecido en la Unión Europea y se base en el cumplimiento de los requisitos antes mencionados; el certificado reconocido o el proveedor de servicios, que se reconocen en el territorio italiano, en virtud, de cualquier tratado bilateral o multilateral celebrado por la UE con terceros países u organizaciones internacionales[809].

Por otro lado, en Irlanda y Malta, reconocen las firmas digitales extranjeras (certificados reconocidos, según la terminología de la Unión) como equivalentes a las firmas nacionales, siempre que satisfagan los demás requisitos jurídicos. En el caso de Austria y Luxemburgo el reconocimiento está sujeto a verificación nacional. En el caso, de Polonia este está sujeto a una decisión de la autoridad nacional. Esta tendencia a insistir en alguna forma de verificación nacional, justificada, en general, por una

[808] BIEREKOVEN, C; BAZIN, P; y KOZLOWSKI, T.: "Electronic Signature in Germany, French and Polish Law Perspective", *Digital evidence and electronic signature law review,* octubre, 2004, núm. 1, pág. 7 – 13.
[809] Disponible en: http://www.clizio.com/S3/docum/FirmaDigitaleENon.pdf (última visita: 14/3/2014).

legítima preocupación, acerca del grado de fiabilidad de los certificados extranjeros, conduce en la práctica a un sistema de discriminación de los certificados extranjeros por razón de su origen geográfico[810].

En España, el reconocimiento transfronterizo ha de tratarse desde la perspectiva del Artículo 14 de la Ley 59/2003, de firma electrónica. Este Artículo es resultado de la transposición literal del Artículo 7 de la Directiva, dando lugar a un régimen restrictivo de reconocimiento, optándose, como en los casos anteriores, por supervisar y controlar para dar seguridad. De esta manera, nace una limitación al reconocimiento intracomunitario de los certificados emitidos por los prestadores de servicios de certificación establecidos fuera de la Unión europea.

Si bien, la Ley Modelo sobre Firma Electrónica contempla que el origen no habría de determinar el reconocimiento de los efectos jurídicos de la firma electrónica o el certificado electrónico, sino que sería su fiabilidad técnica la que determinase la viabilidad y, así, su eficacia jurídica, fundamental para promover la economía y eficiencia del comercio internacional.

Las disposiciones europeas y, en su transposición, las disposiciones españolas, niegan el reconocimiento automático, sin tener en cuenta las cualidades técnicas del certificado, exigiendo garantías, con la consiguiente imposición de barreras, para la competencia internacional prestadores de servicios de certificación situados en terceros países.

El Prof. Illescas considera que además de contrario a la libertad de comercio, resulta perjudicial para los empresarios establecidos en la Unión; pues, si los europeos atribuyen crédito a firmas electrónicas amparadas por certificados que luego no se consideran equivalentes, porque los Estados en su emisión no se adecuan a ninguno de los criterios de equivalencia internacional prevenidos en este Artículo, los grandes perjudicados serán los propios empresarios europeos, que confiaron en un certificado que se puede declarar jurídicamente inválido, aunque técnicamente haya funcionado

[810] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 156 y ss.

satisfactoriamente. Al negársele a éste la aplicación del principio de equivalencia funcional no será fácil fundamentar una demanda ante una jurisdicción europea, sobre la base de una firma electrónica amparada en un certificado no equivalente[811].

La equivalencia internacional de certificados en la Ley de Firma Electrónica española, al igual que en el resto de Europa, solo se hace extensible a los certificados reconocidos; es decir, a los certificados definidos en el Artículo 3 de la misma ("la firma electrónica avanzada basada en un certificados reconocido y que se genera mediante un dispositivo seguro de creación de firma"); en definitiva, la firma equiparable a la firma manuscrita.

Esta firma es la basada en el Artículo 5,1 de la Directiva de firma electrónica, a la que no se le atribuye ninguna definición en particular y que ha de ajustarse al contenido desarrollado en los Anexos I, II y III de la Directiva[812], criterios incorporados en nuestra Ley en el Capítulo II, Título II, que tiene por rubrica "los certificados reconocidos" y, que finaliza, precisamente, con el Artículo 14. Por ello, parece como si el legislador nos estuviera indicando, entre otros, los requisitos que ha de tener una firma reconocida extranjera, en referencia al primero de los apartados del citado Artículo.

La firma electrónica reconocida, es un tipo de firma basada en una tecnología PKI, que como se vio, anteriormente, es una tecnología compleja, que rompe uno de los principios que se pretende instaurar a nivel internacional: la neutralidad tecnológica, principio que se transgredió ya en la Directiva.

De la misma manera, nos encontrarnos con un problema de equivalencia jurídica, que determinara la finalidad del certificado reconocido extranjero. El problema se soluciona con el "sistema voluntario de certificación"[813] (Artículo 14, a) LFE), regulado en los Artículo 26 a 28 LFE, que contemplan la posibilidad de que los prestadores de servicios de certificación sometan a certificación sus operaciones. Se pretende que, de

[811] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 106.
[812] COMISIÓN EUROPEA: *Informe sobre la aplicación de la Directiva 1999/93/CE, de la Comisión al Parlamento, por la que se establece un marco comunitario para la firma electrónica*, Bruselas, 2008. Disponible en: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=2006&nu_doc=120 (última visita 14/3/2014).
[813] Que si bien se recoge en la Directiva y demás leyes europeas, desaparece con el Reglamento.

acuerdo con las prácticas aprobadas por la Unión Europea, se reconozca que el prestador de servicios cumple con todos los requisitos legales exigidos para el desenvolvimiento de su actividad. Así, se trata de la certificación de certificadores[814], con lo que garantiza el cumplimiento directo por parte del prestador no comunitario de unos requisitos que se le exigen para dar confianza y seguridad al sistema, lo cual supone una aplicación del criterio que se establece en la Ley Modelo sobre Firma Electrónica, en su Artículo 12,1, en el que se recoge la necesidad de establecer una fiabilidad técnica, que será el factor que determine el efecto jurídico de la firma electrónica.

De esta forma, se establece este procedimiento de acreditación, para que sirva como sello de garantía de la prestación de servicios, en aras de incrementar la confianza de los destinatarios. Como objetivo del mismo se fija como objetivo, vía Artículo 26,1 LFE, que una entidad cualificada, pública o privada, emita una declaración a favor de un prestador de servicios de certificación, que implica el reconocimiento de que este cumple los requisitos exigidos a la prestación de servicios que ofrece al público; es decir, certifica el cumplimiento de las obligaciones que impone la Ley de firma electrónica[815].

No obstante a lo anterior, debemos dejar claro, que si bien hemos hablado de un sistema de acreditación voluntario, para los prestadores de servicios de certificación no comunitarios, es obligatorio, por exigencias del Artículo 14 LFE. Para los prestadores de servicios comunitarios, este sistema de acreditación, sí es voluntario, dada la imposibilidad de condicionar el desarrollo de esta actividad a la previa acreditación del prestador de servicios; esto es, la prohibición de que puedan existir condicionamientos o autorizaciones administrativas previas, tal y como se recoge en el Artículo 5,1 LFE, por transposición del Artículo 4 de la Directiva de firma electrónica. Aunque es así, en teoría, ya que, indirectamente, todo el entramado regulador va hacia este sistema de acreditación voluntario, si se quiere competir en el mercado con un buen producto, será necesario estar acreditado[816]. En definitiva, se trata de un sistema con un carácter de

[814] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 107.
[815] MÁRQUEZ LOBILLO, P.: "Prestación de servicios de certificación en la LFE", *Revista de la Contratación Electrónica*, núm. 47, Marzo, 2004, pág. 23.
[816] MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de la Contratación Electrónica*, núm. 15, Abril, 2001, pág. 37.

calidad, con un sistema mixto; pues, la acreditación puede darse por una entidad cualificada de carácter público o privado, pero en cualquier caso, ¿quién asumirá la responsabilidad del certificado que en última instancia acredita?; ¿quién responderá?; ¿qué tipo de responsabilidad si cada Estado dispone de régimen de responsabilidad distinto?

La existencia de los sistemas voluntarios de acreditación surge de la necesidad de llegar a un compromiso, dentro de la Unión Europea, para permitir a prestadores de servicios de certificación no habilitados, el ejercicio de los derechos derivados que le son propios. Su finalidad es la obtención de un nivel reforzado de prestación de servicios. No hay problema, en principio, en referencia a la firma electrónica reconocida, en tanto que su contenido es uniforme en todos los Estados de la Unión Europea, pero la firma electrónica avanzada no lo es, lo que supone una incertidumbre difícil de superar. Ante un control y una supervisión *ex post,* como dice la Directiva Europea "hasta que haya recaído la decisión positiva administrativa"[817]; está claro que se deja en manos de los prestadores de servicios de certificación el cumplimiento de las obligaciones y, con ello, recae una responsabilidad incierta, en tanto que no ha sido objeto de armonización. En definitiva, ni los usuarios ni el propio prestador tienen la certeza necesaria para actuar en el tráfico jurídico.

Este procedimiento es la forma de dar fiabilidad a las transacciones que se realicen, pero a la vez puede suponer una discriminación tecnológica y de la propia equivalencia funcional; pues, ya sabemos de la prescripción técnica de la tecnología PKI, establecida en la Directiva y, por incorporación de la misma, en España y demás Estados. Como ya decía la Secretaría de la CNUDMI "una legislación nacional con orientación tecnológica dificulta más que promueve la utilización de las firmas electrónicas en el comercio internacional" y ello con independencia de que este sistema voluntario de certificación contribuya a un aumento de la competencia en el sector[818].

[817] Artículo 2,13 de la Directiva 1999/93/CE.
[818] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.91.

Prueba de ello es que países de la Unión Europea, como por ejemplo Holanda[819], que en su legislación referente a firma electrónica, utiliza distintos métodos de autentificación de firma, incluyendo el sistema PKI[820]. Asimismo, la segunda posibilidad o exigencia del Artículo 14 LFE ("el certificado esté garantizado por un prestador de servicios de certificación establecido en un Estado miembro") abre la vía del reconocimiento transfronterizo a través de la autonomía de las partes, tal y como la recoge en su articulado la Ley Modelo de Firma Electrónica en su Artículo 12,5.

Con esta exigencia se hace suficiente el acuerdo de las partes para que se produzca un reconocimiento de firma, pero no por ello más fácil, ya que nos lleva a otro problema: el prestador de servicios comunitario controlará la fiabilidad del certificado reconocido, asumiendo la responsabilidad, regulada en el Artículo 22,2 LFE. Esta remisión se hace, en concreto, a la verificación de la información, incluida y prescrita en el certificado, y al aseguramiento de que el firmante se encuentra en posesión de los datos, de creación de firma, correspondiente a la verificación.

En definitiva, criterios que se definen como actuaciones que ha de realizar el prestador de servicios de certificación como profesional diligente, derivando de ellas su responsabilidad por su incumplimiento. Esta responsabilidad, si entrar a valorar si es o no excesiva, con respecto a terceros, es lo que puede dificultar la exigencia que valoramos, por los motivos esgrimidos por la CNUDMI[821].

Por último, "el reconocimiento de certificados o del prestador de servicios en virtud de un acuerdo bilateral o unilateral entre la Comunidad Europea y terceros países u organizaciones internacionales" (Art. 14, c LFE), que, efectivamente, como dice la Prof. Martínez Nadal, podría resolver el problema del reconocimiento de firma de países más cercanos y a la vez atender al principio de reciprocidad[822]; pero claro está que no ha sido una idea compartida:

---

[819] Disponible en: http://ec.europa.eu/enterprise/sectors/ict/files/netherlands_en.pdf (última visita: 3/9/2014).

[820] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005 pág. 6.

[821] ORTEGA DÍAZ, J. F.: *Firma electrónica y Contrato de Certificación Electrónicos*, Valencia, 2008, pág. 55.

[822] Considerando 25 de la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

a) En primer lugar, por ser una cláusula difícil de realiza,; salta a la vista si nos vamos al Artículo 7,2 de la Directiva, Artículo al que se nos remite desde el párrafo c) del Artículo 14. Con ello, se rompe definitivamente con la esencia de la Ley Modelo sobre Firma Electrónica: la armonización a nivel internacional de la materia; pero, eso sí, nos hace ver la realidad.

b) En segundo lugar, por poner de manifiesto la discriminación de los certificados y prestadores de servicios de certificación extranjeros.

c) En tercer lugar, por ser una cláusula que podría resultar perjudicial, puesto que el acuerdo bilateral o multilateral, que se firme, tendrá que ser válido para todos los Estados Miembros. Sin embargo, la normativa de los Estados miembros, en esta materia, no es del todo uniforme, lo que puede causar perjuicios a los ciudadanos de un Estado miembro.

Esta posición discriminatoria situada en la Directiva, que se mantiene, en parte, con el Reglamento, al considerar el acuerdo internacional como único criterio válido para el reconocimiento de certificados extranjeros, encuentra como contrapunto la situación adoptada por Reino Unido.

De acuerdo con los principios del Artículo 7 de la *Electronic Transaction Act*, las partes pueden decidir la situación jurídica de la firma electrónica entre ellos, en referencia clara a la cuestión del reconocimiento transfronterizo de certificados y firmas electrónicas. Así, acercándose al marco jurídico establecido en Estados Unidos, prevé un sistema de reconocimiento basado en la fiabilidad de los certificados emitidos por los prestadores de servicios de certificación. De esta forma, establece que el Secretario de Estado puede de revisar el ejercicio de las actividades de certificación de proveedores de servicios que se establezcan en el Reino Unido y que emiten certificados reconocidos al público, examinando toda las circunstancias relacionadas con el ejercicio de tales actividades (Artículo 8).

De este modo, Reino Unido solamente se ha limitado, de acuerdo con la Directiva de la UE, a poner en práctica un marco jurídico para la utilización de la firma

electrónica en toda la UE, sin restringir la circulación de los productos de firma electrónica que se ajusten a la Directiva, dando el mismo tratamiento a un servicio de certificación emitido por un prestador establecido en otro Estado miembro, ya que no pueden imponer requisitos adicionales sobre el uso de la firma electrónica que constituyan un obstáculo para los servicios transfronterizos y para los ciudadanos.

5.5. Propuestas internacionales para mitigar obstáculos al reconocimiento de las firmas electrónicas

5.5.1. La Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales

La CNUDMI en su tendencia a tratar de superar los problemas surgidos, con el fin de que una firma electrónica, basada en un certificado emitido por un prestador de servicios de certificación autorizado, pueda operar en el foro, elaboró la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales en 2005. A través de ella, se trata de dar valor jurídico a las Leyes Modelos, a la vez que eliminar los obstáculos jurídicos que se oponen al uso de las comunicaciones electrónicas.

El Artículo 20 de la Convención, bajo su encabezamiento "Comunicaciones intercambiadas en el marco de otros instrumento internacionales", dispone que la Convención se aplique también al empleo de comunicaciones electrónicas, relacionadas con la formación o ejecución de un contrato, que venga regido por una de las Convenciones que el propio Artículo determina en su apartado segundo.

Con este Artículo se trata de ofrecer una solución a los obstáculos jurídicos con que tropieza el comercio electrónico en los instrumentos internacionales existentes, de

forma que se evite la necesidad de enmendar los distintos Tratados internacionales[823]. De esta forma, se produce una situación atípica en dos sentidos[824]:

a) Se delimita el ámbito de aplicación de una Convención en función de la aplicación de otras Convenciones.

b) Estas resultan indirectamente modificadas, ya que sin modificación formal, se permite incluir supuestos, en principios no contemplados, en referencia al uso de las comunicaciones electrónicas.

La Convención de 2005 se aplica al modo de empleo de las comunicaciones electrónicas en relación con la formación y/o cumplimiento de un contrato (Artículo 1,1); es decir, formación y ejecución de un contrato (no a las comunicaciones electrónicas bursátiles o financieras, etc. excluidas en el Artículo 2,2), sin tener en cuenta la nacionalidad ni el carácter mercantil o civil de las partes del contrato.

Partiendo del ámbito de aplicación de la Convención, hemos de hacer dos precisiones: por un lado, la Convención de 2005 se aplica a las partes cuyos establecimientos estén en distintos Estados; estos es, mensajes electrónicos intercambiados entre partes cuyos establecimientos estén en Estados contratantes diferentes, aun cuando uno de esos Estados no sea contratante[825], en la medida que la Ley de un Estado contratante fuese aplicable a la operación de que se trate; por otro, la Convención de 2005 permite a los Estados contratantes expandir sus disposiciones a otros instrumentos internacionales en los que el Estado contratante sea o no parte del mismo (Artículo 20), lo que lleva a que tengan que ser aplicados e interpretados conforme a la Convención de 2005, facilitándose la aplicación de lo previsto en los Convenios internacionales, en un entorno electrónico, al que no siempre se encuentran acomodados.

---

[823] OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, pág. 45-88.

[824] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 235.

[825] PERALES VISCASILLAS, Mª P.: "Publicidad y Formación del contrato: Convención de UNCITRAL sobre la utilización de las comunicaciones electrónicas en los contratos internacionales, 2005", *Revista Electrónica de la Contratación*, núm. 72, junio 2006, pág. 5.

De esta forma, la regla contenida dentro del Artículo 20 debe interpretarse de forma conjunta con el Artículo 1, referente al ámbito de aplicación, con el fin de evitar la más que probable crítica a la suerte de la unilateralidad, que supondría el planteamiento contrario. Podemos decir que no se imponen reglas de un Convenio a otro Estado que no forme parte de él, sino que tan solo se autodelimita el ámbito de aplicación de la Convención de 2005, en tanto que integrante del ordenamiento nacional señalado aplicable, por el sistema de Derecho internacional privado del Estado del foro, a determinadas situaciones mercantiles internacionales.

Este planteamiento no es automático, pues según se indica en la Nota Informativa de la Secretaría de la CNUDMI[826]: "Los párrafos 1 y 2 presuponen que todo Estado Contratante incorporará a su Derecho interno una disposición que ordene a sus órganos judiciales que recurran al régimen de la Convención para resolver toda cuestión jurídica suscitada por el empleo de mensajes de datos en el contexto de otros convenio internacionales".

Por consiguiente, no se trata de enmendar o modificar ningún convenio, tratado o acuerdo internacional, con independencia de si figura o no en la lista del párrafo 1, ni tampoco se trata de dar una interpretación auténtica del texto de ninguno de esos instrumentos, sino que se trata de eliminar obstáculos jurídicos que el texto actual de los convenios internacionales pudieron imponer al comercio electrónico, lo que resulta lógico conforme a lo dispuesto en el derecho internacional público y en el Convenio de Viena de los Tratados de 1969.

Y no lo hace, porque si se enmendara o modificara un convenio podrían contrariar en alguna medida el objeto y el fin del convenio o tratado, de tal forma que su conclusión y su aplicación haría incurrir a los Estados parte en un acuerdo *inter se* en responsabilidad internacional frente a los demás Estados parte[827].

---

[826] CNDMI/UNCITRAL*: Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de la Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, párr. 290.

[827] MONCAYO, VINUESSA, GUTIERREZ POSSE: *Derecho Internacional Público*, Buenos Aires, 1990, págs. 126 y ss.

Precisamente, la Convención no se centra sólo en la interpretación de los términos utilizados en otros instrumentos, tratando de enunciar reglas de derecho sustantivo que permitan una aplicación eficaz de esas Convenciones internacionales en un entorno electrónico.

A la Convención se le da una aplicación de carácter general y transversal, ofreciendo soluciones prácticas para problemas, que se sustancian en el uso de los medios electrónicos de comunicación en la celebración de contratos internacionales. Y lo hace proyectándose sobre la plantilla resultante de la Convención de Viena de 1980 y con los principios cardinales de la Ley Modelo sobre Comercio Electrónico (1996) y la Ley Modelo sobre Firmas Electrónicas (2001)[828].

Así, teniendo en cuenta que una convención o tratado internacional supone una cierta unidad, relativamente cerrada y suficiente en sí misma, al margen de la relación de normativa necesaria, hay supuestos en los que se establece entre unos y otros acuerdos una concatenación fáctica. Así, la Convención de 2005, como la Convención de Viena de 1980, recurre en ocasiones al criterio de "acuerdos que regulan la misma materia"; es decir, que además de la conexión formal establecida, hay otras que necesariamente surgen de la identidad del objeto entre acuerdos, que pueden ser formalmente distintos.

El estudio del proceso de integración comunitaria europea enseña que aunque haya acuerdos comunitarios todo recibe una unidad en el derecho comunitario y, en su caso, consiste uno de los refinamientos de la unidad de esta técnica de integración.

La Jurisprudencia de la Haya reconoce, que el principio de interpretación de una regla internacional, debe ser interpretada en contemplación de las circunstancias que concurrieron en su constitución y los efectos jurídicos deben ser medidos por el entorno jurídico vigente en el momento de su aplicación[829].

[828] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág. 229.
[829] Disponible en: http://www.un.org/es/icj/ (última visita 14/3/2014).

En consecuencia, la Convención de 2005 se inserta en un marco normativo y sus distintos elementos evolucionan, acompasadamente, de tal modo que la mutación que se produzca repercute a los demás, por lo que esa expansión, en principio, no produce problemas.

No obstante, el empleo de Internet, como medio para la celebración de contratos internacionales, no modifica, normalmente, la determinación de la ley aplicable, como sería el caso de los Artículos 3 a 6 del Convenio de Roma de 1980.

Sin embargo, las peculiares características de la contratación por Internet hacen que la localización de las relaciones jurídicas en un ordenamiento estatal con base a los criterios típicos empleados por las reglas de conflicto en la materia, como el lugar de celebración del contrato, lugar de ejecución de las obligaciones, el domicilio de alguna de las partes, etc. pueden resultar inapropiados, de tal forma que la falta de adecuación de estos criterios puede generar una dificultad en su concreción[830].

Por ejemplo, en términos de perfección del contrato a través de medios electrónicos es internacionalmente aceptado que la oferta es aceptada desde el momento en que la aceptación es recibida por el oferente sin que sea necesario conocimiento de la misma.

Asimismo, hay ordenamientos que aceptan el recurso de la vía electrónica, en el marco de ciertas categoría de operaciones, imponiendo requisitos especiales para su empleo, como puede ser el tipo de firma electrónica utilizada, mientras en otros países adoptan un enfoque más liberal, por razón de la cual, puede suceder que ciertas materias puedan estar sujetas a requisitos especiales o, incluso, excluidas en algunos países, mientras que en otros países no lo están.

Así, por un lado, la Directiva 2000/31/CE señala contratos que no pueden celebrarse por vía electrónica, pudiendo darse el caso de que terceros Estados autorizasen la realización de estos mismos contratos y/o que los mismos Estados miembros excluyan materias y otros no, como consecuencia del carácter voluntario de

[830] MIGUEL ASENSIO, P.A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 419.

la Directiva en esa exclusiones; por otro, la Directiva 1999/93/CE sobre firma electrónica y la transposición, que se hace posteriormente, de la misma, en cada uno de los Estados miembros, nos ratifica lo anterior.

Hemos de tener en cuenta que, el planteamiento del Artículo 20 a los instrumentos de derecho internacional privado comunitario resulta compleja si no imposible: una interpretación literal de este Artículo excluye del ámbito de aplicación material instrumentos supraestatales que no tengan carácter convencional (con independencia de su denominación), siendo los Reglamentos y Directivas de la Unión Europea técnicamente actos de Derecho comunitario europeo y no Convenios internacionales, siendo únicamente aplicable al Convenio de Roma de 1980

Por ello, si las partes, en virtud de la autonomía de la voluntad (Artículo 3 de la Convención de 2005) declararan aplicable a los contratos internacionales que se celebren bajo el paraguas de la Convención de 2005, sin que los Estados fuesen parte del mismo, ¿qué pasaría en tal caso si la normativa aplicable no está adecuada para la celebración del contrato a través de medios electrónicos?

Las partes, en virtud de la autonomía de la voluntad, tan usada en el derecho internacional, para la configuración del contenido obligacional del contrato, son libres para pactar la aplicación al acuerdo de las reglas que tengan por conveniente (Aplicación indirecta).

Ante esto, el Artículo 19, 1 – b) de la Convención de 2005, prevé una limitación eventual del ámbito de aplicación de la Convención, de tal forma que todo Estado podrá declarar que solo aplicará la Convención a determinados contratos si las partes, en dicho contrato, han convenido que su régimen será aplicable a las comunicaciones electrónicas que vayan a intercambiar. Con ello, se reduce la aplicabilidad de la Convención y se priva a todo Estados, que se valiera de ella, de un régimen supletorio uniforme aplicable a las comunicaciones electrónicas intercambiadas entre partes en un

contrato internacional, cuyo texto no prevea todo los pormenores que están resueltos en el régimen de la Convención[831].

Pero, ¿y si la Convención expandiera su aplicación a otros instrumentos internacionales?

Si acudimos a los Convenios o Tratados Internacionales en los que los Estados sean parte, podemos observar en el propio Artículo 20 de la Convención de 2005 una norma de conflicto, o cláusula de conflicto[832], como se denomina el conflicto de Tratados en el Derecho internacional, pudiendo ofrecer una solución funcional y realista a una situación privada de Derecho internacional, determinando la Convención de 2005 qué ordenamiento ha de regir dicha situación.

Estaríamos hablando de una norma de conflicto como el renvío, utilizado como mecanismo de respeto del principio de unidad del ordenamiento jurídico, entendiendo el Derecho internacional como un todo unitario[833]. En este sentido la CNUDMI[834], en la elaboración de esta Convención, tuvo presente la necesidad de evitar que hubiese dos regímenes para la formación de contratos: el régimen uniforme de contratos de la Convención de 2005 y un régimen diferente, no armonizado, que rigiera la formación de contratos por medio de cualquier otro.

5.5.2. Trabajos en curso: la Ventanilla Única (*Single Window*)

En el comercio internacional, las empresas, normalmente, tienen que someterse a grandes volúmenes de información y documentos para cumplir con los requisitos nacionales exigidos para importar y los aspectos reglamentarios relacionados con el tránsito y la exportación. Esta información y documentación tienen que ser presentados

---

831 CNDMI/UNCITRAL*: Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de la Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, párr. 280 y ss.

832 ZAPATERO MIGUEL, P.: "Sistemas jurídicos especiales", *Revista Española de Derecho Internacional*, Vol. LVII - 2005, págs. 187 y ss.

833 CALVO CARAVACA, A. L. y CARRASCOSA GONZÁLEZ, J.: *Derecho internacional privado*, Granada, pág. 300 y ss.

834 CNDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de la Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, párr. 53 y ss.

de acuerdo a las formas específicas que requiere el propio sistema estatal al que se acude.

Los requisitos exigidos son grandes y conllevan un gran coste para su cumplimiento, pudiendo constituir una gran carga para los Gobiernos y la comunidad empresarial y, por tanto, pueden ser un serio obstáculo para el desarrollo del comercio internacional.

En este contexto surge la Ventanilla Única (*Single Windows*) que se define como un mecanismo de facilitación que permite a las partes involucradas, en el comercio y el transporte, alojar información estandarizada y documentos en un sólo punto de entrada, para cumplir con todos los trámites de importación, exportación y tránsito. Si la información es electrónica, solo será remitida una vez. (*Single Window is defined as a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, expert, and transitrelated regulatory requirements. If information is electronic, then individual data elements should only be submitted once*)[835].

Estamos ante una herramienta con la que se quiere permitir el envío de información electrónica una sola vez, ante una única entidad, para cumplir con todos los requerimientos del comercio exterior. Esto es posible a través de la simplificación, homologación y automatización de los procesos de gestión. De esta manera, en términos prácticos, la Ventanilla Única tiene como objetivo agilizar y simplificar los flujos de información entre el comercio y el Gobierno, aportando beneficios significativos para todas las partes involucradas en el comercio transfronterizo. Se trata de dar lugar a una armonización y, con ello, facilitar el intercambio de los datos pertinentes a través de sistemas de Gobierno, con lo que redunda en beneficio de todas las partes involucradas en el comercio transfronterizo[836]. De esta forma, la armonización y la interoperabilidad

[835] UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005, pág. 6. (ECE/ TRADE/352, July, 2005).
Disponible en: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf (última visita: 14/3/2014).
[836] LUDDY, B.: "Session IV: The International Single Window: A Legal Framework View of the Path to Paperless Global Trade Development", *UNCITRAL Colloquium on Electronic Commerce*, 14 - 16 de febrero, 2011, Nueva York.

desempeñan un papel importante en el éxito final de la Ventanilla Única, desde una perspectiva internacional.

Para conseguirlo, la CNUDMI con la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y Las Leyes Modelo sobre Comercio Electrónico y Firma Electrónica, proporcionó un conjunto importante de normas internacionales en el campo del comercio electrónico, que ha dado lugar a un entorno jurídico ideal para el desarrollo de los negocios electrónicos.

Unas de las áreas clave de la Ventanilla Única, a nivel nacional e internacional, son las operaciones relacionadas con el intercambio de información. Por ello, las cuestiones sobre autenticación e identificación, en el entorno electrónico, resultan muy importantes. Por este motivo, resulta importante centrarse en el uso de las firmas electrónicas[837], para avanzar en un comercio electrónico internacional uniforme. No obstante, se ha observado que, las legislaciones nacionales, en particular, suelen centrase en las firmas digitales.

Cuando se adopta una infraestructura legal para el uso de la firma electrónica, es importante tener en cuenta que tipos de transacciones se realizan y el marco en el que se realizan; pues, una firma digital no es más que un tipo de firma electrónica. En este contexto, las empresas hacen negocios internacionales con otras y, a menudo, se ven en el entorno jurídico de un país en particular, teniendo que determinar el nivel de riesgo

---

Disponible en: http://www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010program.html (última visita: 14/3/2014).

[837] Decisión de la Comisión de 16 de octubre de 2009 por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las "ventanillas únicas", con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior que en su considerando 3 y 4 nos dice que "Para respetar la obligación de simplificar los procedimientos y trámites y facilitar el uso transfronterizo de las «ventanillas únicas», los procedimientos por vía electrónica deben basarse en soluciones sencillas, en particular en lo que se refiere al uso de firmas electrónicas. El marco comunitario de la firma electrónica se creó en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. A fin de que del uso transfronterizo de las firmas electrónicas avanzadas basadas en un certificado reconocido resulte eficaz, debe reforzarse la confianza en estas firmas electrónicas con independencia del Estado miembro en que esté establecido el firmante o el proveedor de servicios de certificación que expida el certificado reconocido. Esto podría conseguirse ofreciendo más fácilmente en una forma confiable la información necesaria para validar las firmas electrónicas, y en particular la información relativa a los proveedores de servicios de certificación que están supervisados/acreditados en un Estado miembro y a los servicios que presta. Es necesario garantizar que los Estados miembros pongan esta información a disposición del público mediante un modelo común, a fin de facilitar su uso y garantizar un nivel de detalle apropiado que permita a la parte receptora validar la firma electrónica.

que puede tener que asumir si se deciden a entrar en relaciones comerciales con las empresas de ese país.

Se demuestra, así, que la equivalencia funcional y de neutralidad tecnológica resultan importantes para el desarrollo del comercio electrónico mundial y se han convertido en principios fundamentales[838], que hay que respetar. Por esto, es importante prestar atención a los tipos de firmas electrónicas y las medidas de autenticación[839] que se pueden y deben utilizar en cualquier país, para dar lugar a un entorno jurídico del comercio electrónico interoperable.

Por consiguiente, con la Ventanilla Única se trata de buscar enfoques legislativos interoperables, fijando como principio fundamental la neutralidad tecnológica y al observar las transacciones transfronterizas buscar procesos que se fijen de manera no discriminatoria.

En este contexto, resulta importante, en el establecimiento de un entorno jurídico necesario para la implementación de Ventanilla Única, la identificación de las leyes y sus restricciones, con el fin de posibilitar los cambios que pueden ser necesarios, con el fin de facilitar la presentación electrónica de datos, a fin de facilitar la aplicación de la firma electrónica[840].

De esta forma, resulta decisivo revisar[841] los aspectos legales relativos a la legislación sobre privacidad y las leyes de protección de datos, asociados al desarrollo

[838] PONTEN, J.: "Session IV: Single Window Solutions - Best Practice and Challenges for the Future", *UNCITRAL Colloquium on Electronic Commerce*, 14 - 16 de febrero, 2011, Nueva York.
Disponible en: http://www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010program.html (última visita: 14/3/2014).
[839] UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005, pág. 30 (ECE/ TRADE/352, July 2005).
Disponible en: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf (última visita: 14/3/2014).
[840] LUDDY, B.: "Session IV: The International Single Window: A Legal Framework View of the Path to Paperless Global Trade Development", *UNCITRAL Colloquium on Electronic Commerce*, 14 - 16 de febrero, 2011, Nueva York.
Disponible en: http://www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010program.html (última visita: 14/3/2014).
[841] UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nuena York, 2005, pág. 27. (ECE/ TRADE/352, July 2005).

de la Ventanilla Única, incluyendo la presentación de información por parte de los comerciantes, el intercambio de información entre las diferentes autoridades gubernamentales y organismos y, especialmente, las cuestiones relacionadas con el uso de la firma electrónica.

En este sentido, la Unión Europea, ha establecido obligaciones de simplificación administrativa, impuestas a los Estados miembros en el Capítulo II de la Directiva 2006/123/CE y, en particular, en sus Artículos 5 y 8, que incluyen la obligación de simplificar los procedimientos y trámites aplicables al acceso a actividades de servicios y su ejercicio con la obligación de garantizar que los prestadores de servicios puedan realizar fácilmente dichos procedimientos y trámites a distancia por vía electrónica, a través de las Ventanillas Únicas. Esta Directiva viene a establecer qué simplificación de trámites y procedimientos debe ser posible a través de las fronteras, gracias al uso transfronterizo de las firmas electrónicas avanzadas, basadas en un certificado reconocido que resulte eficaz entre Estados miembros con arreglo al Artículo 8.

Ante la problemática que se presentada en torno a la firma electrónica, se ha realizado una revisión del marco regulatorio de la firma electrónica, que se recoge en la Directiva 1999/93/CE, a través del Reglamento, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que la deroga.

Finalmente, en relación con la *Single Window*, la Cámara de Comercio Internacional, recientemente, ha puesto en práctica los denominados Certificados de Origen[842], un documento, que identifica el origen de las mercancías que se exportan[843] y

Disponible en: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf (última visita: 14/3/2014).

[842] Disponible en: http://www.iccwbo.org/chamber-services/trade-facilitation/certificates-of-origin/ (Última visita: 24/4/2014).

[843] En 2003 el Grupo de Trabajo por la Federación Mundial de Cámaras de Comercio estableció el primer Certificado Internacional de Origen Electrónico, a través del cual se establecieron unas directrices, con el fin de mejorar las prácticas internacionales para los procedimientos de emisión. De esta manera se examinó detenidamente los problemas recientes y la importancia de obtener el reconocimiento de estos documentos y sus firmas digitales por todas las administraciones de aduanas. De esta forma han detectado una serie de áreas problemáticas claves, como son: los datos de administración (recopilación, distribución, modificación, eliminación, acceso, retención y archivo), la privacidad y la seguridad; la gestión de la identidad; los datos personales; la información confidencial en el comercio y datos de la competencia; la propiedad intelectual; la responsabilidad, cumplimiento de la ley y de resolución de conflictos, etc.

que es requerido por la aduana, como una de las bases fundamentales para la aplicación de tasas arancelarias. La expedición de los certificados de origen y la certificación correspondiente de los documentos de exportación fue regularizado, en virtud de lo dispuesto en el Convenio de Ginebra de 1923, para la simplificación de las formalidades aduaneras.

La Federación Mundial de Cámara de Comercio es el foro global de la Cámara de Comercio Internacional, que sirve para acreditar a las cámaras de comercio, para la emisión de certificados de origen (CO), a través de procesos estándares y las directrices de certificación internacional de certificados de origen y de un programa internacional de capacitación en CO.

Estas directrices de certificación son: la de apoyar procedimientos transparentes de emisión, asegurar la emisión independiente y responsable, dar credibilidad a los certificados de origen emitidos por las cámaras de comercio y elevar el nivel de aceptación por parte de las administraciones aduaneras y la comunidad comercial.

De esta forma, se trata de incrementar la aceptación de los CO electrónicos por parte de las aduanas y la entrega de certificados de origen preferenciales por parte de cámaras competentes, a través de alianzas con las aduanas. Se trata de crear una Ventanilla Única[844], que pueda simplificar y hacer más eficiente y eficaz el proceso de envío de datos, para operaciones de importación y exportación. Por ello, esta Ventanilla Única permitirá el intercambio de información, entre los organismos gubernamentales, en relación con las transacciones comerciales internacionales, creando las condiciones propicias para una Ley internacional, que regule esta materia, que constituye uno de los principales retos para los países que establecen este tipo de instalaciones nacionales[845]. Muchas son las cámaras de comercio, que ofrecen certificados en origen en línea, para

[844] XUE, H.: Challenges and opportunities: a regional agreement electronic, *UNCITRAL Colloquim*, febrero, 2011, pág.7.

[845] Naciones Unidas ha elaborado el "UNeDocs Projects**":** un proyecto de la Comisión Económica para Europa que se puso en marcha en el año 2000 para analizar los problemas documentales de la cadena de suministro y desarrollar soluciones. Con el apoyo de los gobiernos, asociaciones industriales e institutos de investigación, el proyecto desarrolló estándares internacionales de importancia para la documentación en el comercio internacional y para el comercio electrónico, tales como "United Nations Layout Key and UN/EDIFACT".
Disponible en: http://www.unece.org/fileadmin/DAM/trade/workshop/wks_capbld/unedocs_summary.pdf (Última visita: 24/4/2014).

acelerar el proceso de solicitud y expedición; al mismo tiempo que, proporcionan un entorno de documentación más seguro. De hecho, los sistemas incluyen características de seguridad, como la verificación en línea de la autenticidad de los certificados.

CAPÍTULO SEXTO: LAS PARTES INTERVINIENTES EN LA TRANSACCIÓN

6.1. La responsabilidad de las partes intervinientes en las transacciones electrónicas

Respecto a la responsabilidad, en el contexto de las firmas electrónicas, pueden plantearse distintas cuestiones en función de la tecnología y la infraestructura de certificación utilizada. Así pues, surgen cuestiones complejas, en particular, en los casos en que se encargue de la certificación un tercero especializado, como un prestador de servicios de certificación; en este caso, habrá, esencialmente, tres partes, que serán: el prestador de servicios de certificación, el firmante y el tercero que confía. En la medida en que sus actos u omisiones causen daño a cualquiera de las demás o contravengan sus obligaciones expresas o implícitas, cada una de ellas podrá ser tenida por responsable o perder el derecho a invocar responsabilidad frente a la otra.

La función principal de la responsabilidad es servir de instrumento a la reparación del daño causado, proporcionando al perjudicado un marco adecuado para obtener una compensación adecuada; pero sin olvidar que, también, puede cumplir otro tipo de funciones, ya sea preventiva, ya sea punitiva. La función preventiva de la responsabilidad civil cobra gran relevancia, cuando el análisis jurídico se enfoca desde un punto de vista económico. De esta manera, cuando los daños derivados de unas determinadas relaciones jurídicas presentan o pueden presentar una especial importancia económica o cuando pueden suponer un riesgo para el equilibrio general, la eficiencia económica y la seguridad jurídica[846] son necesarias tenerlas muy en cuenta.

La responsabilidad, que se deriva de las prácticas de las entidades de certificación[847], es una cuestión esencial desde el punto de vista económico-social y empresarial. Por ello, muchos países, con el fin de de conseguir el adecuado marco de seguridad y confianza, consideran necesario realizar un marco de control sobre

[846] LAFUENTE SUÁREZ, M.: "La Ley de firma electrónica y la responsabilidad civil de los prestadores de servicios de certificación", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2007, núm. 13-1.
[847] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 59/2003 de Firma Electrónica*, 2009, págs. 335 y ss.

determinadas firmas electrónicas. Dentro de dicho control, destaca el de la actividad de los prestadores de servicios de certificación, como pieza clave de todo el sistema de firma electrónica. Así, los titulares y los usuarios de certificados, especialmente, si son consumidores, no van a participar en un mercado, cuyas condiciones económicas y legales son oscuras e inciertas; menos aún, las entidades certificadoras comerciales, cuya difusión, depende en gran medida, del grado de riesgo asociado con la actividad empresarial que ejercitan, potencialmente alto, para las entidades de certificación sin legislación específica, sometidas, en muchos casos, a las normas generales de responsabilidad.

Por ello, los diferentes niveles de la responsabilidad pueden constituir un obstáculo para el reconocimiento transfronterizo de las firmas electrónicas, afectando a su operatividad, por varias razones: podría ser que los prestadores de servicios de certificación no quieran reconocer certificados extranjeros o las claves expedidas por prestadores de servicios de certificación extranjero, cuya responsabilidad o cuyas normas en materia de diligencia, sean menos estrictas que las suyas; los usuarios de métodos de firma y autentificación pueden temer que la imposición de una responsabilidad y una expectativa de diligencia menor al prestador de servicios de certificación extranjero, limite los recursos con que puedan contar, en caso de falsificación o defraudación[848].

Asimismo, se plantea una especial inquietud en lo que respecta a las relaciones entre las diversas entidades certificadoras, ya que, en muchos casos, nos encontramos ante la necesidad de que entidades certificadoras, sustancialmente equivalentes, reconozcan mutuamente los servicios prestados, de tal manera que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad y/o seguridad de los certificados. De esta forma, nos encontramos con que, en la mayoría de las leyes nacionales, hay normas establecidas en referencia a cuándo y cómo se considerarán equivalentes los certificados internacionales, expedidos por prestadores de servicios establecidos en Estados distintos al suyo.

[848] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, pág. 86 y ss.

Ante esta situación, pasamos a estudiar las diferentes disposiciones adoptadas en relación con las normas de conducta, atendiendo a los distintos enfoques de responsabilidad que se han adoptado, respecto a las partes que intervienen en la propia transacción.

6.1.1. Establecimiento de normas de conducta y régimen de responsabilidad para todas las partes: la CNUDMI/UNCITRAL

La Ley Modelo sobre Firma Electrónica identifica todas las partes, que pueden llegar a participar en la transacción: el firmante (Artículo 8 – Proceder del firmante), la autoridad certificadora (Artículo 9 – Proceder del prestador de servicios de certificación) y el tercero que confía (Artículo 11 – Proceder de la parte que confía en el certificado).

De esta forma, fija diferentes criterios para evaluar las distintas formas de actuar, dejando en manos del derecho nacional, todo lo relativo a las consecuencias del incumplimiento de sus obligaciones y fundamento de la responsabilidad de las partes, que utilicen sistemas de firma electrónica; es decir, se establecen regímenes de conducta y los requisitos del certificado[849]. Si se incumple las pautas de conducta establecidas, se incurrirá en responsabilidad. Estas pautas de conducta, si observamos la relación lógica establecida en los Artículos 8 y 9 (y con ellos los Artículos 10 y 11), giran en torno en torno a la diligencia y, por ello, en la fiabilidad.

Como sabemos, esta estructura triangular es reflejo de la decisión adoptada por la CNUDMI de centrarse en cuestiones y terminología relativas a la infraestructura de clave pública, que se relaciona con la existente entre las distintas de partes. Sin embargo, esta afirmación no es del todo cierta; pues, realmente, lo que se trató de establecer es un régimen abierto que diera cabida, no sólo a la tecnología imperante en la época, sino también a la que pudiera surgir con posterioridad, optándose por la neutralidad tecnológica. En este sentido, resulta evidente que centrarse en las funciones, que se llevan a cabo en un entorno de infraestructura de clave pública y no hacerlo en un modelo concreto, facilita, también, el desarrollo de una norma de neutralidad,

[849] MADRID PARRA, A: "La identificación en el comercio electrónico", *Revista Electrónica de la Contratación*, núm. 15,2001, pág. 3 -60.

respecto de los medios técnicos utilizables, en la medida en que en la tecnología de firmas electrónicas, que no sean de infraestructura de clave pública, se prestan funciones análogas[850].

Con los rápidos cambios que afectan a los aspectos técnicos y comerciales del comercio electrónico, junto con el papel, que, actualmente, desempeña la autoreglamentación en el comercio electrónico, de ciertos países, puede dificultar el consenso sobre el contenido de esas reglas. Por ello, los Artículos se redactaron de modo que representen un "código de conducta" mínimo para las diversas partes. Por ello, en relación con el objeto de dejar suficientemente claro que los efectos de los Artículos 8, 9 y 11 consisten, simplemente, en establecer principios, sin ocuparse de ninguna de las consecuencias que pudieran derivar de esos principios, con arreglo al derecho aplicable[851]; pues, a lo largo de los trabajos preparatorios de la Ley Modelo se concluyó, en lo que concierne a las entidades prestadoras de servicios de certificación y los firmantes, que los derechos y obligaciones de las partes vendrán determinados por el acuerdo entre las partes, a reserva de lo que disponga la Ley aplicable[852].

Por consiguiente, en relación con los mencionados criterios mínimos, se señala la obligación, general, del prestador de servicios de certificación de utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables y de actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas; además, se espera que actúe con diligencia razonable, para cerciorarse de que todas las declaraciones materiales que haya hecho, en relación con el certificado, sean exactas y cabales. Respecto al firmante, debe actuar con diligencia razonable, con respecto a sus datos de creación de firma. Cuando el firmante sepa o deba saber que dichos datos han dejado de ser seguros, deberá dar aviso inmediato a cualquier persona que, según razonablemente prevea, pueda verse afectada por haber considerado fiable la firma electrónica o prestar servicios que la refrenden. Igualmente, se espera que el firmante actúe con diligencia razonable, para cerciorarse de que todas las declaraciones que haya

[850] CNUDMI/UNCITRAL: *Guía para la incorporación de la Ley Modelo de la CNUDMI para las Firmas Electrónicas (2001) al derecho interno*, Nueva York, 2002, párr.32 y ss.
[851] CNUDMI/UNCITRAL: *A/CN.9/484 - Informe del Grupo de Trabajo sobre Comercio Electrónico acerca de 38º período de sesiones*, Nueva York, 12 a 23 de marzo de 2001, párr. 67 y 68.
[852] CNUDMI/UNCITRAL: *A/CN.9/483 - Informe del grupo de trabajo sobre comercio electrónico acerca de la labor de su 37º período de* sesione, Viena, 25 de junio a 13 de julio de 2001, párr. 25, 26, 113 y 137.

hecho, sean exactas y ciertas. En cuanto al tercero que confía en el certificado se espera que tome las medidas precisas para verificar la fiabilidad de la firma electrónica, así como tomar medidas razonables para verificar su validez, suspensión o revocación y, además, cualquier limitación que le afecte[853].

La responsabilidad puede plantear distintas cuestiones en función de la tecnología y la infraestructura de certificación utilizadas. Pueden surgir problemas complejos, en particular, en los casos en que se encargue de la certificación a un tercero especializado, como un prestador de servicios de certificación. Por ello, como cuestión de redacción, en relación con los prestadores de servicios de certificación, se convino que se reemplazaran palabras: "Los autores de la Ley Modelo se esmeraron en no requerir" por las palabras "La Ley Modelo no requiere"[854].

6.1.2. No establecimiento de disposiciones expresas sobre normas de conducta o responsabilidad: Estados Unidos

En Estados Unidos, tanto en la E-Sign como en la UETA, se hace notar la ausencia de disposiciones acerca de la conducta o responsabilidad del firmante, destinatario (tercero que confía) o de las entidades que prestan servicios de certificación[855], lo que no es una casualidad, debido al enfoque que se le ha dado a las Leyes. De esta forma, se muestra conciencia de que el establecimiento de distintos regímenes de responsabilidad puede obstaculizar el reconocimiento transfronterizo de las firmas electrónicas.

No obstante, ambos marcos normativos contienen disposiciones relativas a la protección del consumidor, a través de las cuales se les protege de empresas que pudieran aprovechar los registros electrónicos para eludir las leyes, que requieren que los consumidores reciban ciertas informaciones y documentos, tales como: la confirmación de la transacción; declaración de los términos y condiciones de la

[853] CNUDMI/UNCITRAL: *Guía para la incorporación de la Ley Modelo de la CNUDMI para las Firmas Electrónicas (2001) al derecho interno*, Nueva York, 2002, párr. 78 y ss.
[854] CNUDMI/UNCITRAL: *A/CN.9/484 - Informe del Grupo de Trabajo sobre Comercio Electrónico acerca de 38º período de sesiones*, Nueva York, 12 a 23 de marzo de 2001, párr. 67 y 68.
[855] MIYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *ScienceDirect Review,* enero, 2007.

transacción; copia de su contrato, por si surgiera alguna controversia; información, sobre cualquier derecho de cancelación de la operación dentro de un plazo determinado (Section 101 (c)(1)(c)(ii), prevención del fraude al consumidor) [856], etc.

Hasta este punto, todo es lógico, si tenemos presente, que en el comercio electrónico, se plantean cuestiones relativas a la protección de datos y los derechos humanos en lo tocante al almacenamiento y divulgación de datos y que, además, se requieren normas para proteger a los consumidores del riesgo de la utilización privada de datos y la posibilidad eventual de robo de identidad.

Teniendo en cuenta el consejo de la Secretaría de la CNUDMI[857], en la medida en que una excesiva protección de los consumidores y usuarios de certificados electrónicos, podría ser un obstáculo al comercio, llegamos a un punto problemático en Estados Unidos; pues, la E-Sign y la UETA, si bien son similares en muchos aspectos, no lo son en la forma de tratar a los consumidores[858].

La E-Sign contiene importantes medidas de protección a los consumidores, que están ausentes en la UETA. Las medidas se encuentran en la Sección 101 (C) de la E-Sign, transcritas en el *United State Code*, concretamente, en el Título 15, Capítulo 96, Subcapítulo I, § 7001. Además, la E-Sign[859] contempla que los Estados puedan añadir protecciones adicionales de consumo, siempre que sean compatibles a lo previsto en las Leyes federales. Asimismo, previene que un Estado puede "modificar, limitar o sustituir" partes de la E-Sign, con respecto a la UETA. De esta forma, teniendo en cuenta que la E-Sign proporciona una mayor protección a los consumidores que la UETA, se debería prestar especial cuidado para que los Estados que promulguen la UETA no modifiquen las protecciones en lo referente al consumidor, establecidas en la E-Sign.

---

[856] FEDERAL TRADE COMMISSION AND DEPARTMENT Of COMMERCE*: Electronic Signature in Global and National Commerce Act. The Consumer Consent Provision in Section 101 (c) (1) (c) (ii).* junio de 2001.
Disponible en: http:// www.ftc.gov/os/2001/06/esign7.htm#N_23_ (última visita: 24/9/2014).
[857] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr.205.
[858] Disponible en: http://www.consumersunion.org/finance/e_sign.htm#_ftn1 (última vista: 5/5/2014).
[859] HILLEBRAND, G; SAUNDERS, M.: *E-Sing and UETA, what should states do now?* Consumers Union, 2006, pág.3 y ss.

Así, en las transacciones de consumo, por un lado, la E-Sign requiere un proceso específico y electrónico antes de la notificación electrónica, de manera que puede sustituir un aviso escrito por la forma electrónica requerida legalmente; por otro, la UETA establece que las partes se comprometen a realizar transacciones por medios electrónicos, sin especificar cómo debe ser probado el acuerdo dimanante, de manera que en los Estados en los que se ha adoptado la UETA, el acuerdo se determinara del contexto y de las circunstancias, es decir, se determinará transacción por transacción[860].

De la E-Sign se desprende que el consentimiento expresado por el consumidor debe mostrar la capacidad del firmante a la hora de obtener el acceso a la información. Si acepta recibir las comunicaciones por medios electrónicos, pero no puede demostrar su capacidad para obtener acceso a la información en la forma que establece, las cláusulas especiales del contrato de consumo serán ineficaces[861]. Si bien un contrato electrónico celebrado por un consumidor no se le puede negar validez por el sólo hecho de haber sido firmado electrónicamente, siempre debe demostrarse, razonablemente, que el consumidor puede o ha podido tener acceso a la información en formato electrónico y que este formato se ha utilizado para proporcionar la información. El incumplimiento de las obligaciones de información a los consumidores conlleva sanciones de conformidad con la legislación aplicable, sanciones que varían de un Estado a otro.

De esta forma, parece que las disposiciones establecidas para la defensa de los consumidores, recogidas en la E-Sign, están funcionando satisfactoriamente, facilitando el comercio electrónico, el uso de los registros electrónicos y las firmas al mismo tiempo. Sin embargo, es cierto que la falta de coordinación crea inquietud, debido a la diferencias y a la falta de interacción entre esta norma y la UETA[862]. Además, en un

[860] WITTIE A. ROBERT; WINN, K. J.: *Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA*, 2007.
Disponible en:
http://www.law.washington.edu/Directory/docs/Winn/Electronic%20Records%20and%20Signatures.htm (última visita: 7/5/2014).

[861] SPYRELLI, C.: "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", Journal of Information, Technology and Law, vol. 2, núm. 2, 2002, pág. 3 – 59.

[862] KNAUS, J.P.; FOLEY, T. E.: "Electronic Records & Signatures: The federal E-Sign Act and Michigan UETA place them on legal par with their paper and ink counterparts", *Michigan Bar Journal*, Julio, 2001.
Disponible en: http://www.michbar.org/journal/pdf/pdf4article293.pdf (última visita: 27/5/2014).

entorno en el que se multiplican los contratos internacionales, donde, a nivel mundial, la cooperación en materia de consumidores es casi nula, el entrono creado por la legislación de Estados Unidos crea mayor inseguridad si cabe, al haber diferentes regulaciones en los diversos Estados de la Unión.

En opinión de algunos autores, con la aprobación de la E-Sign, se perdió la razón principal para que los Estados promulguen la EUTA. De esta manera, los Estados deberían considerar la disminución de las competencias recogidas en la UETA, en favor de la E-Sign. De no hacerlo, si un Estado promulga la UETA, debería optar por subordinar lo establecido en su norma a la E-Sign, o sería mejor combinar la UETA con un Capítulo que agregara las protecciones al consumidor, según E-Sign, ayudando a construir un marco idóneo para establecer confianza y fomentar el uso del comercio electrónico[863]. Sin embargo, la Conferencia Nacional del Comisionado para Leyes Estatales Uniformes, autora de la UETA, que tiene representantes en todos los Estados, está haciendo todo lo posible para que se opte por la UETA. No obstante, si el Estado opta por la UETA, debe tratar por todos los medios, no "modificar, limitar o sustituir" las protecciones del consumidor previstas en la E-Sign; pues, de lo contrario, se estaría dando un pasos atrás.

6.1.3. Establecimiento de normas de conducta y régimen de responsabilidad aplicables únicamente al prestador de servicios de certificación: la Unión Europea

La Directiva 1999/93/CE sobre la firma electrónica, en su objetivo de facilitar el uso de las firmas electrónicas reconocidas, trata de estimular y promover la actividad de los proveedores de servicios de certificación, mediante la definición de sus necesidades esenciales y su responsabilidad, con el fin de apoyar el proceso de construcción de confianza para los consumidores y las empresas que dependen de los certificados. Para ello, establece normas de responsabilidad, en exclusividad, para estos proveedores de servicios en el Artículo 6.

[863] BUCKLEY, J. S.; TANK, M., BUCKLEY KOLAR LLP: *Electronic Signatures and Records Under ESIGN, UETA and SPeRS,* 2007.
Disponible en: http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ElectronicSignatures.pdf (última visita: 7/5/2014).

Para entender el sistema de responsabilidad establecido para los proveedores de servicios de certificación, que figura en la Directiva, es necesario centrarse: por un lado, en el Considerando 22, que viene a decirnos que los "proveedores de servicios de certificación, que ofrecen servicios de certificación al público, están sujetos a la normativa nacional en materia de responsabilidad", declarando la intención del legislador europeo de no hacer frente a la responsabilidad de proveedores de servicios de certificación en la Directiva; por otro lado, en el Artículo 6, establece, de manera detallada, los criterios de responsabilidad de los proveedores de servicios de certificación, pero solo los que emiten certificados cualificados.

De una interpretación conjunta del Considerando 22 y el Artículo 6, se observa que éste Artículo, solo se aplica si el certificado ha sido expedido como certificado reconocido (o cualificado), de tal manera que si este certificado no lo fuese sería irrelevante respecto a la Directiva, debiendo entrarse a valorar la normativa nacional. Dicho con otras palabras, las reglas del sistema de responsabilidad de los proveedores de servicios de certificación, que emiten certificados reconocidos, caen bajo el ámbito de aplicación de la Directiva, mientras que la responsabilidad de los proveedores de servicios de certificación, que emiten certificados no reconocidos, se rigen por las Leyes nacionales.

De esta manera, la Directiva obliga a los Estados miembros a garantizar, como mínimo, que el prestador de servicios de certificación que expida al público un certificado, presentado como certificado reconocido o que garantice al público tal certificado, sea responsable del perjuicio causado a cualquier entidad, persona física o jurídica, que confíe razonablemente en el certificado, por lo que respecta a[864]:

a) La veracidad en el momento de su expedición, de toda la información contenida en el certificado reconocido y a la inclusión en el certificado de toda la información prescrita para los certificados reconocidos.

[864] Artículo 6,1 de la Directiva 1999/93/CE, del Parlamento y del Consejo, de 13 de Diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

b) La garantía de que, en el momento de la expedición del certificado, obraban en poder del firmante, identificado en el certificado reconocido, los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado.

c) La garantía de que los datos de creación y verificación de firma pueden utilizarse complementariamente, en caso de que el prestador de servicios de certificación genere ambos; salvo que el prestador de servicios de certificación demuestre que no ha actuado con negligencia.

Así, mientras la Ley Modelo sobre Firma Electrónica opta por prever normas de conductas, como criterios para evaluar la actuación de las partes; la Directiva prevé la responsabilidad solo del prestador de servicios de certificación, respecto del que considera necesaria una armonización[865]. El legislador comunitario ve a los prestadores de servicios de certificación como un elemento trascendental en establecimiento de la seguridad. Por ello, al objeto de proteger la confianza de terceros, los sitúa ante la responsabilidad por el perjuicio causado a cualquier entidad o persona física que confíe razonablemente en el certificado.

Sin embargo, la Directiva no impone ningún deber al prestador de servicios de certificación, salvo que emita certificados reconocidos, en cuyo caso deberá seguir las instrucciones contenidas en el Anexo II de la Directiva; es decir, la determinación de la Directiva es la de fijar la responsabilidad, que se circunscribe, únicamente, al prestador de servicios de certificación de firma electrónica reconocida, dejando fuera cualquier otro tipo de responsabilidad, que deberá ser recogido por los distintos ordenamientos jurídicos nacionales de los Estados miembro. Con ello, en el mencionado, Artículo 6 establece un grado de mínimo de responsabilidad del prestador[866], que los Estados podrían aumentar, lo que situaría a los prestadores de servicios de certificación de un país, en desventaja frente a los otros Estados miembros.

[865] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 86.
[866] BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, núm.3, vol. 4, 2004, págs.211-242.

Vemos que la responsabilidad de las autoridades de certificación debería haber quedado claramente definida, para garantizar ese grado de seguridad, que se quería conseguir para promover la asimilación de las firmas digitales. Principalmente, hay dos cuestiones relativas a la responsabilidad de las autoridades de certificación, donde se plantea diversidad normativa[867]: en las inexactitudes o falsedades contenidas en el certificado y en que la autoridad de certificación no revoca un certificado no válido[868]. En virtud del contrato y el derecho de daños, la responsabilidad potencial de la entidad de certificación puede ser complicada; pues, va a depender del valor de las transacciones para las que pueda utilizarse la firma digital.

Ante esto, si tenemos en cuenta, que en la mayoría de casos, se puede plantear la posibilidad de que el prestador de servicios de certificación limite su responsabilidad potencial frente a la parte que confía, la responsabilidad se ve que está sujeta a restricciones aún mayores. Esto ocurre a menudo, ya que la parte que confía no tiene obligaciones contractuales ante el prestador de servicios de certificación, ni ante el firmante. Así, en la medida en que la parte que confía pueda tener derechos en el ámbito extracontractual, frente al prestador de servicios de certificación o el firmante, quizá esas partes no tengan modo de limitar su responsabilidad, porque en la mayoría de ordenamientos jurídicos, esto requeriría informar, debidamente, de dicha limitación a la parte que confía, dado que el prestador de servicios de certificación desconoce la identidad de la parte que confía antes de que se produzca el daño; por ello, tal vez no pueda aplicar un sistema eficaz de limitación de su responsabilidad. Estamos ante un problema típico de los sistemas abiertos, en los que unos desconocidos interactúan sin contacto previo, que deja al firmante desprotegido ante consecuencias potencialmente devastadoras[869]. Depender de responsabilidad contractual y extracontractual es una cuestión problemática, ya que depende de las leyes de las jurisdicciones particulares y asegura poca certeza.

[867] De esto se deduce se deduce una posible vulneración del principio de libre prestación de servicios consagrado en los Artículos 49 a 55 del TCE, principio que determina la aplicación del principio de no discriminación entre proveedores por razón de su origen, lo que exige poner en particular atención en la regulación estatal de las condiciones de acceso y establecer el reconocimiento de los prestadores de servicios constituidos válidamente en otro Estado miembro.

[868] FEN LIM, Y.: "Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability", *Singapore Journal of International & Comparative Law*, núm.7, 2007, págs. 183-200.

[869] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 206.

La Directiva opta por una responsabilidad claramente subjetiva, basada en la culpa del prestador de servicios, ya sea esta contractual o extracontractual. Pudiendo éste ser responsable de sus actos frente al usuario (titular del certificado) o frente al tercero de confianza, que puede verse perjudicado por cualquier acto u omisión de aquél[870]. Esta característica sobre la responsabilidad se puede apreciar en el apartado primero del Artículo 6 de la Directiva ("la responsabilidad causada a cualquier entidad o persona física o jurídica"), que, solo puede enmarcarse dentro de una tecnología PKI, porque únicamente puede aplicarse a ésta[871] y, además, se hace aplicable, por el tenor literal del Artículo, como hemos comentado antes, a las firmas electrónicas reconocidas.

Esta responsabilidad solo se excluye si el prestador de servicios demuestra que no ha actuado con negligencia. Con ello se recoge una inversión de la carga de la prueba, por el simple hecho de que es quien mejor puede demostrar su buen hacer. Todo ello se encuentra regulado en la Ley Modelo sobre Firma Electrónica, pero con un ligero matiz: mientras que la Ley Modelo, en su Artículo 9, exige una diligencia razonable al prestador de servicios[872], la Directiva obliga a los Estados, estableciendo una responsabilidad, genérica, pero rígida, en cuanto a sus mínimos a cumplir; esto es, la Ley Modelo pretende, como idea fundamental, fijar una correlación razonable entre el valor del certificado emitido y las obligaciones con la subsiguiente responsabilidad[873], mientras la Directiva establece que el prestador de servicios es responsable por el daño causado a cualquier entidad que confíe, razonablemente, en el certificado reconocido, salvo si prueba que no ha actuado con negligencia.

---

[870] IPR HELPDESK: *"Estudio sobre firma electrónica"*, Proyecto financiado por la Comisión Europea. Dirección General de Empresas e Industria en el sexto programa Marca sobre IDT de la Unión Europea. Pág. 5

[871] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 86.

[872] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 87.

[873] MADRID PARRA, A.: "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica* (Dirs. Etcheverry R.A. e Illescas Ortiz, R.), Buenos Aires, 2010, pág.219

La negligencia[874], particularmente su ausencia, es un criterio que absuelve a una autoridad de certificación de la responsabilidad, que podría asociarse con la diligencia debida en muchos casos. En cualquier caso, es predicable la negligencia como concepto central en la determinación de la responsabilidad de una autoridad de certificación. La cuestión lo situamos en que el concepto de negligencia no es un concepto interpretado de manera uniforme en todos los Estados, causando confusión ante los distintos grados que puede obtener.

El enfoque de responsabilidad adoptado combina una variante a la responsabilidad objetiva del prestador de servicios de ciertos actos o declaraciones falsas con un sistema que permite a la autoridad de certificación limitar su responsabilidad, en determinadas circunstancias. Por un lado, con la inversión de la carga de la prueba, por la inexactitud de la información consignada en el certificado o falta de cumplimiento de los requisitos para la emisión del certificado reconocido; y por otro, para proporcionar seguridad a los prestadores de servicios de certificación y favorecer su desarrollo (Artículo 6,3); se recoge la importancia de que las legislaciones nacionales establezcan la posibilidad de que todo prestador pueda consignar en un certificado reconocido limites, en cuanto a sus posibles usos o en cuanto al valor límite de las transacciones que puedan realizarse con el mismo, de manera que cuando se supere estos, el prestador no responderá de los posibles daños que ese empleo pueda causar[875]. Estos límites suelen ser de dos tipos: límites a los tipos de operaciones, para los que puedan usarse ciertos certificados o clases de certificados y límites al valor de las operaciones, para las que puede usar cierto certificado o clases de certificados[876]. En ambos casos, se dice expresamente que el prestador de servicios no responderá de los "daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites incluidos en el mismo".

Precisamente, la Directiva en el Artículo 6 apartados 3 y 4, obliga a los Estados miembros a que velen porque el prestador de servicios pueda consignar en un certificado reconocido "límites en cuanto a sus posibles usos, siempre y cuando los

[874] BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, 2004, núm.3, vol. 4, págs.211-242.
[875] MIGUEL ASENSIO, P.A.: "Regulación de la firma electrónica: balance y perspectiva", *Direito da Sociedade da Informaçao,* Coímbra, 2004, págs. 115 – 143.
[876] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 99.

límites sean reconocibles para terceros" y "un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles por terceros"[877]. Por un lado, el límite en cuanto a sus usos, se establece para fijar la responsabilidad, al emitirse el certificado para un uso determinado, esta limitación deberá hacerse de forma expresa, clara e inequívoca, facilitándose con ello, que los terceros conozcan o puedan conocer esta limitación[878]; por otro, el límite de las cuantías se establece para determinar la responsabilidad a un importe máximo, relacionado con el valor de las transacciones realizadas con el certificado. Sin embargo, no se establece un tope de la responsabilidad en la que pueda incurrir un prestador de servicios, siendo los Estados miembros los que determinen la misma.

Ante los problemas suscitados en la Directiva, surge un nuevo marco jurídico para los proveedores de servicios de certificación, a través del Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que trata de unificar la responsabilidad de estas entidades a la vez que aportar mayor seguridad jurídica.

En primer lugar, trata de hacerlo, cambiando la denominación de los prestadores de servicios de certificación por proveedores de servicios de confianza[879], con este cambio terminológico parece querer llevar a un cambio de rumbo[880]. Con este cambio se intenta dar cercanía al utilizarse el término confianza, como una forma de referirse a las relaciones entre personas. Si uno confía en otro, el primero espera una buena conducta, una esperanza o, incluso, una seguridad firme de que se va a hacer algo bien. En nuestra opinión, si bien el proveedor de servicios de confianza y el prestador de servicios de certificación vienen a ser lo mismo, lo que se pretende es atraer la atención del usuario, creando un clima de confianza en un entorno en el que es necesario, por las

[877] BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, 2004, núm.3, vol. 4, págs.211-242.
[878] IPR HELPDESK: "Estudio sobre firma electrónica", *Proyecto financiado por la Comisión Europea. Dirección General de Empresas e Industria en el sexto programa Marca sobre IDT de la Unión Europea*, pág. 6.
[879] Por lo general, se interpretaba qué "entidad" se refiere a los terceros que confían, y la Directiva se ha aplicado en este sentido en todos los Estados de la Unión Europea, excepto en dos: Hungría y Dinamarca. (BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, 2004, núm.3, vol. 4, págs.211-242.
[880] LÓPEZ JIMENEZ, D.: "Iniciativas empresariales de regulación del comercio electrónico: el supuesto de la península Ibérica", *Revista de la Contratación Electrónica*, núm. 114, 2011, págs. 3 a 49.

características que tiene el marco tecnológico que se desarrolla. Por ello, se quiere dar a entender como un proveedor de servicios, con sus acciones y sus caracteres, puedan hacer que las personas, física o jurídica, vean en Internet un universo más o menos confiable.

De esta manera, el nuevo marco regulatorio decreta los principios relativos a la responsabilidad y carga de la prueba de los proveedores de servicios de confianza, tanto cualificados como no cualificados (Artículo 13). En un principio, en la propuesta realizada por la Comisión, se distinguía claramente entre ambos[881], fijando un entorno propio para cada uno, aunque finalmente se eliminó dicha referencia, para pasar a hacer una referencia genérica a ambos prestadores de servicios, para luego centrarse con mayor rigor en los prestadores de servicios de confianza cualificados. Asimismo, añade "que se aplicarán con arreglo a las normas de responsabilidad nacionales", dando carácter normativo a lo que antes se situaba, en el mencionado, Considerando 22 de la Directiva.

Esta responsabilidad se basa en el Artículo 6 de la Directiva 1999/93/CE y extiende el derecho a compensación de los daños causados por un proveedor de servicios de confianza negligente, que incumple las buenas prácticas de seguridad, lo que desemboca en una violación que tiene un impacto importante sobre el servicio. De esta forma, los proveedores de servicios de confianza serán responsables de los perjuicios directos causados a cualquier persona física o jurídica, en razón del incumplimiento de sus obligaciones. Siendo responsables indirectos los organismos de supervisión que los Estados miembros deberán establecer en sus territorios.

El sistema de responsabilidad vuelve a centrarse, exclusivamente, en el establecimiento de normas aplicables a los proveedores de servicios de confianza, estableciendo la inversión de la carga de la prueba a éste, debiendo demostrar que en su actuación no hubo culpa ni negligencia. Se indican requisitos y obligaciones que deben cumplir todos los proveedores de forma que se garantice un alto nivel de seguridad de cualquier servicio o producto de confianza que se preste o utilice. Los proveedores de

[881] COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, (COM (2012) 238 final).

servicios deben aplicar estos de requisitos de seguridad, con el fin de evitar cualquier tipo de riesgo relacionado con sus actividades, a fin de promover la confianza de los usuarios (Artículo 19 del Reglamento).

Se adopta un criterio genérico de responsabilidad mínimo, que se sitúa en las medidas técnicas y organizativas que utilicen para gestionar los riesgos de seguridad. De tal modo que, la redacción del Artículo parece dar una directriz a los Estados miembros, para poder fijar la responsabilidad en casos concretos, o un consejo a los propios proveedores de servicios de confianza, para que establezcan sus propios códigos de conducta.

Lo único que no deja lugar a dudas es la obligación de comunicar, sin demoras indebidas y cuando sea posible, dentro de un plazo de 24 horas (Artículo 19,2), así como la obligación de notificar cualquier violación de la seguridad o merma de la integridad, que tenga un impacto significativo en el servicio de confianza prestado y en los datos personales correspondientes, al organismo de supervisión que corresponda.

Por otro lado, en los Artículo 19 y siguientes, se establece la responsabilidad exclusiva para los proveedores de servicios de confianza que emiten certificados cualificados, siendo responsables directos de los perjuicios causados a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el presente Reglamento. En estos Artículos, se les exige el cumplimiento de una serie de obligaciones positivas, rígidas y taxativas, a la vez que un alto grado de diligencia, que rozan un régimen de responsabilidad objetiva. Sin embargo, el prestador de servicios de certificación cualificado puede quedar exento de responsabilidad si demuestra que actuó con la diligencia debida, pasando a ser responsable la autoridad supervisora.

El Reglamento es claro, rígido y omite ambigüedades que presentaba la Directiva en su articulado, exigiendo conductas que pueden llevar al establecimiento de la confianza de los consumidores en la contratación electrónica. La responsabilidad es de carácter subjetivo basado en con una inversión de la carga de la prueba; es decir, se contemplan actividades de peligro específico, que atribuyen el daño al agente mediante una presunción de culpa que puede ser desvirtuada con la prueba de que actuó con la

diligencia requerida[882]. De esta forma, el prestador debe demostrar que no actuó con negligencia, ya que es quien mejor puede demostrarlo por disponer de la pericia técnica y el acceso a la información pertinente necesaria (de los que posiblemente no dispongan ni el firmante ni los terceros que confían). Quizá se haya optado por un sistema de presunción de culpa, porque se piense que la responsabilidad, basada en la negligencia simple, no sería justa para la parte que confía; pues, tal vez, ésta no disponga de los conocimientos tecnológicos ni del acceso a la información pertinente necesaria, para demostrar que el prestador de servicios de certificación ha actuado con negligencia[883].

La responsabilidad se funda en los riesgos que la actividad crea. La responsabilidad basada en el riego consiste en la obligación de reparar los hechos dañosos producidos por una actividad que se ejerce en el propio interés. De esta forma, se enfatiza que la responsabilidad puede venir por el riesgo que lleva la realización de una actividad o una conducta ilícita, que recae sobre quien crea el riesgo o peligro. Se destaca por ende que se trata de actos ilícitos, pero que generan responsabilidad.

Además, la Comisión, mediante actos de ejecución, podrá establecer números de referencia de norma para sistemas y productos dignos de confianza (Artículo 24,5). De esta forma, se pueden imponer requisitos adicionales a los prestadores y con ellos un mayor grado diligencia, lo que puede restringir el acceso al mercado de proveedores e, incluso, el reconocimiento de proveedores que deseen probar suerte en el mercado comunitario por la vía del Artículo 14 (relativo a "Aspectos internacionales"), donde se describen los mecanismos de reconocimiento y aceptación de los servicios de confianza cualificados prestados por un proveedor de servicios en un tercer país, siempre que se haya celebrado un acuerdo internacional.

A esta restricción podemos sumarle la obligación del proveedor de servicios cualificado, que expide, al público un certificado presentado como cualificado, que verifique, en el momento de su expedición, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado (Artículo 24,1), lo

[882] MEDINA ALCOZ, Mª: *La culpa de la víctima en la producción del daño*, Madrid, 2003, pág. 563.
[883] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 185 y ss.

que puede conllevar limitaciones en el uso transfronterizo de certificados cualificados. En la práctica, visto el régimen de responsabilidad previsto, sólo las Administraciones públicas son las únicas proveedoras de servicios de confianza que se atreven a cumplir con la normativa; asimismo, observamos cómo, de nuevo, vuelve a incidirse en el Derecho nacional y en la identidad, con todo lo que ello supone.

Importante, para entender la responsabilidad que puedan tener los proveedores de servicios, es la obligación que tienen los Estados miembros de crear organismos de supervisión para ambos tipos de proveedores (Artículo 17), introduciendo un mecanismo explícito de asistencia mutua entre los organismos de supervisión (Artículo 18), con el objetivo de facilitar el reconocimiento transfronterizo de los proveedores de servicios de confianza. Se introducen normas sobre las operaciones conjuntas y el derecho de las autoridades de supervisión a participar en estas operaciones. Estos requisitos incluyen una notificación formal a la autoridad nacional de control; además de, presentar informes anuales de auditoría, realizados por reconocidos organismos independientes, para confirmar el cumplimiento de los requisitos establecidos aquí. Solo tras la verificación de los informes, la autoridad nacional de control otorgará el *estatus* de cualificado. Todos los proveedores de servicios cualificados se incluyen en una lista pública de confianza (Artículo 22), En esa lista se definirán las especificaciones técnicas, mantenida por los órganos de control[884].

La inclusión, en una lista de servicios de confianza, significa la admisión del certificado del prestador dentro del ámbito de uso de la lista en cuestión. Esta lista debe cumplir las especificaciones técnicas recogidas en el Anexo de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las Ventanillas Únicas, con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior[885]. El objetivo de esta obligación es mejorar el uso transfronterizo de la firma electrónica mediante el aumento de la confianza en la firma electrónica de otros Estados miembros.

[884] JOS DUMORTIER, J.; VANEZANDE, N.: "Trust in the proposed EU regulation on trust services?" *Computer Law &Security Review*, Vol. 28, Num. 5, octubre, 2012, p. 568 -576.
[885] Disponible en: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm (última visita: 12/5/2014).

6.1.3.1. Alemania

Alemania, en su Ley de firma electrónica, no regula la conducta del firmante ni de la parte que confía, pero si impone obligaciones y responsabilidades a los prestadores de servicios de certificación. De esta forma, sigue los pasos de la Directiva, dedicándose solo y exclusivamente a estas entidades.

La Ley utiliza un régimen de libre prestación de servicios de certificación, aunque, de forma similar a la Ley de Firma Electrónica española, intenta restringir esta libertad, dentro de los límites permitidos dentro de la Directiva. En el Artículo 1,3 de la Ley, se hace uso de potestad otorgada por la Directiva en el Artículo 3,7, que prevé que el uso de la firma electrónica en el ámbito público pueda quedar supeditada a la cumplimentación de requisitos adicionales, siempre que estos requisitos sean objetivos, proporcionados, no discriminatorios y solo puedan hacer referencia a características específicas de la aplicación de que se trate. Por otro lado, ha introducido la posibilidad de una acreditación voluntaria, en términos similares a la Ley española: estableciendo unos requisitos para ejercer los servicios de certificación.

El Artículo 4,2 establece la obligatoriedad de que, los prestadores de servicios de certificación posean seguridad y conocimientos necesarios, así como, cumplan la Ley y el reglamento. Si bien, proclama la ausencia de autorización administrativa en la acreditación, aunque si se necesita, para ejercer la actividad certificadora, obtener una autorización que será emitida por la Autoridad Reguladora de Telecomunicaciones (*Regulierungsbehörde für Telekommunikation*).

Aunque la Autoridad Reguladora no examina su cumplimiento *a priori*; pues, son examinados cada tres años, si condiciona el cumplimiento de estas exigencias a la expedición de la autorización (Artículo 15), ya que con el cumplimiento de estos requisitos puede probarse la seguridad técnica y administrativa necesaria para la emisión de certificados reconocidos, imprescindibles para la existencia de una firma

cualificada[886]. De conformidad, con el Artículo 23 de la Ley, se reconocerán como jurídicamente equivalentes a las firmas electrónicas, basadas en un certificado de un proveedor de servicios de certificación acreditado, en el sentido del Artículo 15,1, si se ha demostrado que se adhieren a los estándares de seguridad.

En lo que se refiere a la responsabilidad de los prestadores de servicios de certificación, como sabemos el Artículo 6 de la Directiva recoge un grado mínimo de responsabilidad del prestador de servicios de certificación, que los Estados miembros podrán aumentar aplicando, un régimen de responsabilidad objetiva o ampliando la responsabilidad a los certificados no reconocidos. Algo que si ocurriera, situaría a los prestadores de servicios de certificación, de los distintos Estados, en una situación de desventaja.

La Ley alemana administra la responsabilidad de estas entidades en el Artículo 11. En este Artículo, se dice que si el proveedor de servicios de certificación no cumple con lo establecido en la Ley o en la reglamento, en virtud del Artículo 24, o si sus productos para la firma electrónica reconocida u otros medios técnicos de seguridad fallan, deberán reembolsar el daño sufrido a terceros por confiar en los datos de un certificado reconocido. Esta responsabilidad no se aplicará si el tercero tenía conocimiento de la inexactitud de la declaración o debería haberla tenido o si el prestador de servicios de certificación no ha tenido la culpa o si un certificado reconocido restringe el uso de la firma, para determinadas aplicaciones según el tipo o el alcance de la transacción, los daños solo se abonará dentro de los límites de las restricciones[887].

Es por esto que, el legislador alemán a considerado necesario hacer una distinción entre la responsabilidad contractual y responsabilidad extracontractual a terceros, basado en el principio de subsidiariedad de la Directiva; es decir, sobre la culpa o negligencia, aunque rechaza la inclusión de la responsabilidad extracontractual de las autoridades de certificación a terceros. Una regla especial de responsabilidad, que no existe en el derecho interno alemán, que supondría superar el nivel necesario para la

[886] CRUZ RIVERO, D.: "Firma electrónica y documento electrónico en la nueva regulación alemana: su adaptación a la normativa comunitaria", *Revista de la Contratación Electrónica*, marzo, 2002, pág. 25 – 50.
[887] Sec. 11 de la SigG.

armonización del mercado interior; si esto se llevara a cabo en todos los Estados miembros se constituiría una armonización de las normas de responsabilidad de los Estados miembros.

Una regulación de la responsabilidad de las autoridades de certificación a terceros crearía un régimen de responsabilidad mucho más estricto del que exige la Directiva. De esta forma, se muestra miedo a un régimen de responsabilidad, que supondría una carga a las entidades europea oferentes de servicios de certificación en europeos, que están en competencia con los proveedores de los sistemas jurídicos de Asia y Estados Unidos[888].

En el Artículo 12, el legislador recoge una limitación a la responsabilidad de las entidades certificadoras, de manera que el proveedor de servicios de certificación debe tener cobertura financiera adecuada para cubrir los daños causados en forma culposa por el funcionamiento de un servicio de certificación. Lo hace para cubrir los daños causados por un hecho que lleva a la responsabilidad del tipo señalado en el Artículo 11, pero lo hace recogiendo cantidades mínimas.

Esta limitación de la responsabilidad se recoge de acuerdo con el Artículo 7,1 de la Ley, respecto de los datos incluidos en la información del certificado en cuanto a "si el uso de la clave de firma se restringe a ciertas aplicaciones cuantitativamente" y el Artículo 11,3 que indica que la responsabilidad de la entidad certificadora solo puede ocurrir en el contexto de una de las limitaciones indicadas. Por lo tanto, la entidad tiene en la mano la forma de limitar la indemnización por daños y perjuicios, respecto de las restricciones sobre el uso del certificado[889].

6.1.3.2. Italia

El ordenamiento italiano sigue los pasos de la Directiva 1999/93/CE, estableciendo un régimen exclusivo de obligaciones y responsabilidad de los

[888] BLOCHER, W.: "Zur Haftung des Zertifizierungsdiensteanbieters nach S 11 Signaturgesetz 2001", *Blocher: Zur Haftung des Zertifizierungsdiensteanbieters*, 2007, págs. 434-449.
[889] HINDELANG, S.: "No remedy for dissapointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Informatica, Law and Technology*, nº 1, 2002.

prestadores de servicios de certificación. Para ello, parte del régimen de libre prestación de servicios de certificación, en cumplimiento con lo establecido por la propia Directiva. No obstante, se puede observar como la libre prestación de servicios de certificación, una vez más, dentro de los límites permitidos, trata de restringirse.

Por un lado, el Artículo 34 establece que las Administraciones públicas pueden actuar como entidades certificadoras en sus relaciones con empresas, ciudadanos u otras administraciones. Al mismo tiempo les otorga la posibilidad de emitir certificados a empresas. Estas administraciones solo podrán emitir certificados reconocidos. Asimismo, obliga a todos los ciudadanos que quieran presentar un documento electrónicamente, ante ellas, a firmarlo digitalmente o a utilizar su DNI electrónico.

De esta manera, al igual que la mayoría de los Estados miembros, sitúan en una posición dominante a los prestadores de servicios públicos, lo que supone limitar la libre circulación de bienes y servicios dentro de la Unión Europea. Dada la posición que ocupa la Administración, el Estado prevé las medidas que considere oportunas en seguridad, para proteger a sus Administraciones públicas, permitido por el artículo 3,7 de la Directiva. Además, dado que cada vez es mayor el número de sistemas de acreditación dentro de los Estados miembros de la UE se presenta un nuevo obstáculo real a la libre competencia.

Por otro lado, el apartado 1 del Artículo 26 nos dice que la actividad de los prestadores de servicios de certificación, establecidos en Italia o en otro Estado miembro, es libre y no requiere autorización previa. Sin embargo, el apartado tercero nos dice que los certificadores, que tengan su establecimiento permanente en otro Estado miembro de la Unión Europea, no se le aplicarán las disposiciones del Código ni las normas técnicas a que se refiere el Artículo 71, aplicándose las normas de transposición de la Directiva 1999/93/CE sobre firma electrónica.

Ante esto, se presenta cierta incertidumbre jurídica en cuanto a la normativa aplicable a la responsabilidad de los propios prestadores de servicios de certificación, pues se viene a establecer la “no aplicación de lo establecido en el Código”. Nos encontramos con un reenvío, figura jurídica que, por su forma de reconocimiento o aparición, despierta inquietud en el Derecho internacional, ya que nos encontramos con

un mecanismo de solución de los conflictos negativos de jurisdicción; es decir, se aplica a aquellos que nacen cuando, en una relación de derecho privado con un elemento extranjero relevante, surgen dos o más legislaciones de distintos ordenamientos jurídicos y que ninguna de ellas se atribuye competencia a sí misma para resolver el asunto, sino que cada una da competencia a una legislación extranjera.

El reenvío se hace a la Directiva, que en su Artículo 4 establece la libre circulación de productos de firma electrónica que se ajustan a esta norma, lo que supone ajustarse a los requisitos establecidos en sus Anexos, con los problemas que plantean y que, además, en cuestión de responsabilidad, reenvía la materia de nuevo a la legislación estatal; es decir, se aplica sólo con respecto a la emisión de certificados reconocidos, no a la responsabilidad por el perjuicio que pueda causar la confianza en un certificado emitido por cualquier entidad. Los prestadores de servicios de certificación que emitan certificados no reconocidos quedarán sujetos a lo establecido en el Decreto Legislativo, surgiendo problemas de reconocimiento transfronterizo de las firmas electrónicas de cualquier nivel ante la falta de concreción y de seguridad jurídica, respecto a la acción de los propios prestadores de servicios de certificación de los demás Estados miembros.

En cualquier caso, si resultase aplicable el Decreto Legislativo italiano, los proveedores de servicios de certificación, sus representantes legales y responsables administrativos, deben cumplir con los requisitos de honorabilidad exigidos a las personas que desempeñan funciones administrativas, de dirección y de control en los bancos[890]. Este requisito da una situación extraordinaria de responsabilidad a todos los prestadores de servicios de certificación; incluso a los que no expiden certificados reconocidos, a quienes también le es aplicable, pues nos remite a otra Ley del ordenamiento jurídico italiano.

[890] VIRILI, C.; CANTONI, C.: "The Italian legislation on digital signatures and the role of Italian banks as Certificate Authorities: A strategic analysis", *Banking (including Insurance Stream): E-Commerce Services*.
Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.7323&rep=rep1&type=pdf (última visita: 26/5/2014).

La responsabilidad de prestador de servicios de certificación[891] se regula en el Artículo 30, indicando que la entidad emisora de certificados reconocidos es responsable, a menos, que pueda demostrar que ha actuado sin negligencia, culpa o dolo, del daño causado a cualquier persona: a) de la exactitud o integridad de la información necesaria para verificar la firma, en la misma fecha de emisión y su integridad con respecto a los requisitos de los certificados reconocidos en el Artículo 28; b) la garantías necesarias para asegurar la identidad del firmante; c) la garantía de que los datos de creación y verificación de la firma puedan ser usados de modo complementario, en los casos en que el certificado generen ambos; y d) la garantía de cumplimiento de las obligaciones establecidas en el Artículo 32, que incluyen una serie de medidas organizativas y técnicas, que deben tenerse en cuenta, para garantizar la seguridad de las operaciones y evitar daños a las partes involucradas en las relaciones jurídicas, en las que estas firmas se utilizan.

De conformidad con el párrafo segundo del Artículo 30, la entidad emisora de certificados reconocidos al público es responsable, ante terceros de buena fe que confíen en el certificado, en relación con el daño causado por el registro extemporáneo de la revocación o la no suspensión, en tiempo, del certificado, a menos que pruebe que actuó sin culpa. De esta forma, el prestador de servicios es responsable frente a terceros que han confiado en el certificado, por los daños causados como consecuencia de la falta o retraso en la grabación (informática), la revocación o suspensión del certificado, según lo requerido por las normas técnicas del Artículo 71, a menos que, una vez más, pruebe que actuó sin culpa.

El párrafo tercero del Artículo 30 recoge la posibilidad de establecer límites de uso o de valor a los certificados. Todo ello a condición de que esos límites sean reconocibles para terceros y estén claramente identificados en el certificado. En este caso, el prestador no se hará responsable de los daños que pudieran causarse.

Ante esta situación, respecto a la responsabilidad, rígida y a la vez restrictiva, del prestador de servicios de certificación, se puede identificar: una responsabilidad contractual, respecto de las obligaciones asumidas por el prestador con sus clientes y a

[891] Disponible en: http://www.digitpa.gov.it/iscrizione-elenco-certificatori (última vista: 19/5/2014).

terceros; pues, se reconoce que los certificados reconocidos pueden contener "límites de uso o límites en el valor de las transacciones reconocibles para terceros y están claramente identificados en proceso de verificación de firmas"; una responsabilidad extracontractual, respecto al producto que erróneamente se ha emitido y que puede causar daños a terceros, ya que se puede suponer la responsabilidad de la certificación, en relación con la primera actividad que se realiza, con el suministro inexacto y que deriva en un daño directo y mediato, respecto de la propiedad y del destinatario final de la transacción.

Por otro lado, al firmante, persona a quien se le asigna la firma electrónica y el acceso a dispositivos para la creación de la firma electrónica, se le obliga a tomar todas las medidas de índole técnica y organizativas necesarias para evitar el daño a otros y para mantener y utilizar el dispositivo de firma (es decir, el hardware y el software que se utiliza para fijar el firma electrónica en un documento electrónico) "con la diligencia de un buen padre de familia" (Artículo 32, párrafo primero, que nos lleva a relacionarlo con el principio general recogido en el Artículo 1227 del Código Civil). Así, el Decreto Legislativo añade una disposición de interés en la que se aprecia la regulación de conducta del sujeto firmante, que a raíz del Artículo 32,1 se le otorga la obligación de custodiar su firma electrónica y de tomar todas las medidas técnicas y organizativas, que considere necesarias para prevenir cualquier daño. Lo que significa la imposibilidad de confiar su firma a cualquier persona para que actúe en su nombre.

El control de los prestadores de servicio de certificación se fija en el Artículo 31 que establece una autoridad supervisora: la CNIPA[892]. Las funciones de esta autoridad se recogen en el Artículo 36 que viene a establecer un régimen para retirar el certificado expedido en el caso de cese de actividades entidad y debe revocar o suspender: a) incumplimiento de una orden de la Autoridad (administrativa o judicial); b) tras la petición del propietario o del tercero con facultades del titular; c) causas de limitación de la capacidad (o de acción) del empresario, por mal uso o por falsificación; y d) en los casos previstos en el Artículo 71, que también se regulan los procedimientos de revocación o suspensión. La revocación o suspensión del certificado reconocido se producirá a la fecha de publicación.

[892] Disponible en: ttp://www.cnipa.gov.it/ (última visita: 19/5/2014).

6.1.3.3. España

La regulación del prestador de servicios de certificación es la que da origen a la mayoría de las normas específicas sobre firma electrónica, en España, como elemento típico en la relación de garante que ostenta, frente al iniciador o firmante y al tercero que confía y como esencia en la infraestructura de clave pública (PKI). De esta forma, a efectos de seguridad jurídica, resulta conveniente su regulación, pues, es el sujeto que hace posible el empleo de la firma electrónica, que equivale a la firma manuscrita.

En el Artículo 2,2 de la Ley de firma electrónica, se define al prestador de servicios de certificación como "la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica".

El prestador de servicios expide certificados electrónicos. Los certificados electrónicos son definidos en el Artículo 6,1 de la Ley como "un documento firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firma a un firmante y confirma su identidad". En palabras del Prof. Plaza Penadés, "son los documentos que relacionan las herramientas de firma electrónica en poder de cada usuario con identidad personal, dándole así, a conocer en el ámbito telemático, como firmante"[893]. La figura del prestador de servicios se crea para garantizar la identidad del emisor del mensaje de datos, asumiendo la responsabilidad de dicha verificación, dotando al sistema de seguridad y confianza para los usuarios[894].

A esta definición legal se le debe añadir lo establecido en el Artículo 5,1 de la Ley de firma electrónica (Artículo 4,1 de la Directiva), en lo que se refiere a la prohibición expresa de someter al prestador de servicios de certificación a servicios de autorización previa, ya que realizará sus funciones en régimen de libre competencia y prohibiendo la imposición de cualquier restricción procedente de cualquier Estado miembro del

[893] PLAZA PENADÉS, J.: "La firma electrónica y su regulación en el derecho español" en *Contratación y comercio electrónico* (Dir. Orduña Moreno, F.J.; coord. Campuzano Laguillo, A.B. – Plaza Penadés, J. (Coords.), Valencia, 2003, pág. 543.

[894] PAREJO NAVAJAS, T.: "Análisis de las figuras esenciales del régimen jurídico de la firma electrónica: la Ley 59/2003, 19 de diciembre, de firma electrónica", *Revista Electrónica de la Contratación*, núm. 70, 2006, pág. 3 - 32.

Espacio Económico Europeo. Dicha prohibición se sustenta en el respeto a los principios del país de origen y reconocimiento mutuo de las legislaciones internas de los Estados miembros, comprendidas en el ámbito normativo, coordinado y consagrado por el legislador comunitario y nacional, en las normas sobre comercio electrónico y firma electrónica[895].

La Ley española, hace una transposición total del articulado de la Directiva 1999/93/CE. Al hacerlo trae consigo los mismos defectos que contiene la mencionada Directiva[896]. Sin embargo, por un lado, incluye en su Artículo 18 obligaciones a cumplir por todos los prestadores de servicios de certificación, mientras la Directiva recoge solo recoge obligaciones para el prestador de servicios de certificación que emite certificados reconocidos; por otro, la Directiva define el certificado reconocido como el certificado que cumple los requisitos establecidos en el Anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el Anexo II[897], mezclando requisitos del certificado reconocido y los deberes que deben cumplir las entidades de certificación, confusión que se traslada a las legislaciones de transposición. Algunas de esas menciones del Anexo II deberían ser requisitos del certificado reconocido y otras exigencias para las entidades de certificación que expidan otro tipo de certificados[898].

Con ello, tal y como comenta el Prof. Cruz Rivero[899], la Ley abre el debate de si todos los deberes de los prestadores de servicios de certificación, que expidan certificados reconocidos, son requisitos para que el certificado sea reconocido. Así, el ambiguo Artículo 11,1 debe entenderse como que todos los deberes establecidos en el Anexo II de la Directiva son requisitos del certificado; pues, lo contrario llevaría a romper la uniformidad en la Unión Europea de los requisitos de los prestadores de servicios de certificación, que emitan certificados reconocidos, y dificultaría el reconocimiento de las firmas electrónicas reconocidas de otros países de la Unión, lo que contraviene la Directiva de firma electrónica. Lo que ocurre es que alguno de los

[895] MÁRQUEZ LOBILLO, P.: "Prestación de servicios de certificación en la LFE", *Revista de contratación electrónica*, núm. 47, Marzo, 2004, pág. 10.
[896] ILLESCAS ORTÍZ: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 145.
[897] Artículo 2,10 de la Directiva 1999/93/CE.
[898] CRUZ RIVERO, D.: *La firma electrónica reconocida. Análisis de los requisitos del artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006, pág. 90.
[899] CRUZ RIVERO, D.: *La firma electrónica reconocida. Análisis de los requisitos del artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006, pág. 91.

deberes establecidos en la Ley, aunque encuentran su fundamento en el Anexo II de la Directiva, son desarrollo del mismo, pudiendo variar este desarrollo de uno a otro Estado. Por ello, resultaría más que dudoso negar la condición de reconocida a una firma electrónica por el hecho de que, cumpliéndose los postulados de seguridad generales de la Directiva, el prestador de servicios de certificación no siga el desarrollo concreto, que de la Directiva, realiza la Ley.

En el Artículo 18 de la Ley se regulan obligaciones que han de cumplir todos los prestadores de servicios de certificación que expidan certificados, ya sean o no reconocidos, siendo deberes recogidos para estos últimos en el Anexo II de la Directiva y, por ello, transpuestos a la Ley en los Artículos 11,1 y 20,1.

Las obligaciones citadas se refieren a: no almacenar ni copiar los datos de creación de firma de la persona a la hayan prestado sus servicios, lo que garantiza que solo el titular de la firma va a tener acceso a los datos de creación de firma, lo que es esencial para que una firma sea considerada avanzada[900]; proporcionar al solicitante antes de la expedición del certificado la información mínima establecida en el propio Artículo de forma gratuita, por escrito o por vía electrónica; mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida, la integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados; garantizar la disponibilidad de los mecanismos de seguridad adecuados.

De esta forma, se obliga al prestador de servicios a la tutela y gestión permanente de los certificados electrónicos que expiden, poniendo por escrito todos los detalles de dicha gestión, en la denominada declaración de prácticas de certificación, así como a mantener un servicio de consulta sobre el estado de vigencia de tales certificados[901].

Además de estas obligaciones, el prestador de servicios de certificación, que emita un certificado reconocido, deberá cumplir las obligaciones especiales recogidas en los

[900] CRUZ RIVERO, D.: *La firma electrónica reconocida. Análisis de los requisitos del artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006, pág. 105.
[901] PAREJO NAVAJAS, T.: "Análisis de las figuras esenciales del régimen jurídico de la firma electrónica: la Ley 59/2003, de 19 de diciembre, de firma electrónica", *Revista de la Contratación Electrónica*, núm. 70, 2006, pág. 3 – 32.

Artículos 12 y 13, con carácter previo, y el Artículo 20, en orden a la comprobación de los solicitantes y la fiabilidad y las garantías de los servicios de certificación que prestan.

Estos prestadores de servicios se encuentran sometidos a una serie de obligaciones enumeradas en los Artículos 12 y siguientes de la Ley: unas, de índole administrativa; otras, propias de la diligencia debida de un ordenado comerciante; otras, componen el contenido imperativo del contrato, que vincula al prestador de servicios de certificación con el iniciador del mensaje de datos de firma electrónica reconocida[902].

Con carácter previo a la expedición del certificado deberán comprobar la identidad y las circunstancias personales de los solicitantes de certificado, con arreglo a lo dispuesto el en Artículo 13, siendo este deber donde se encuentra la razón de ser del prestador de servicios de certificación; es decir, verificar que la información contenida en el certificado es exacta e incluye todas las menciones exigidas por el Artículo 11,2 para un certificado reconocido; asimismo, asegurar que el firmante está en posesión de los datos de creación de firma, correspondientes a los de verificación que obran en el certificado; y, además, garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Además de las obligaciones citadas, el Artículo 20,1 establece otras condiciones con las que ha de contar para el desarrollo de su actividad: demostrar la fiabilidad necesaria para prestar los servicios de certificación; garantizar que pueda determinarse con precisión la fecha y la hora en la que se expidió el certificado o se extinguió o suspendió la vigencia; emplear personal con cualificación, conocimientos y experiencia necesaria para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados, en el ámbito de la firma electrónica; utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirve el soporte; tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de

[902] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 141.

certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante; conservar registrada por cualquier medio seguro, toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante quince años, contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo; y, utilizar sistemas fiables para almacenar certificados reconocidos, que permitan comprobar su autenticidad e impedir que, personas no autorizadas, alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones[903].

A lo dicho, hay que añadir otra obligación, dispuesta en el apartado segundo del Artículo 20: la obligación de disponer de recursos para afrontar el riesgo de responsabilidad. Concretamente se establece la obligación de "constituir un seguro de responsabilidad, por una cantidad de 3.000.000 de euros, para afrontar el riesgo de las responsabilidad por los daños y perjuicios, que pueda ocasionar el uso de certificados que expida".

La doctrina ha criticado el tenor literal de este apartado, por cuanto impone que se garanticen obligatoriamente sólo los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan; pues, parece quedar fuera de la garantía otros supuestos generadores de responsabilidad para la entidad de certificación. No tiene sentido que la Ley restrinja el objeto de la garantía cuando los daños, que puedan ocasionarse a terceros y al propio titular del certificado, puedan, igualmente, provenir de estas otras actuaciones de la entidad de certificación. Por ello, debe ser interpretado de forma amplia este Artículo para, de esta forma, entender que la garantía recogida cubre todo el proceso de certificación y, en general, la responsabilidad de la entidad de certificación, como consecuencia de los daños ocasionados por el negligente incumplimiento de sus obligaciones[904].

[903] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica,* Madrid, 2009, pág. 336.
[904] CRUZ RIVERO, D.: *La firma electrónica reconocida. Análisis de los requisitos del artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006, pág. 142.

Si se incumple, lo comentado anteriormente, los prestadores de servicios de certificación responderán de los daños y perjuicios que causen, a cualquier persona, en el ejercicio de su actividad. El contenido mínimo, obligatorio y rígido recogido en el Artículo 6 de la Directiva y en los Artículos 22 y 23 de la Ley.

La regulación de la Ley se centra en la responsabilidad de los prestadores de servicios de certificación, sin realizar una enumeración de las obligaciones y deberes de las partes; aunque, es posible hallarla a través del Artículo 23 ("Límites de la Responsabilidad de los Prestadores de Servicios"), donde se recogen supuestos de exoneración de responsabilidad de los prestadores[905]. Por ello, la responsabilidad es de carácter subjetivo, en materia contractual y extracontractual, por culpa o negligencia y, por tanto, no objetiva; y, también, con inversión de la carga de la prueba, al establecer que habrá de ser el prestador de servicios de certificación quien haya de demostrar que actuó con la debida diligencia[906],

La Ley, a través del Artículo 23, recoge normas expresas reguladoras de la conducta del firmante electrónico, recogiendo un grado de diligencia relacionado con la posesión, custodia, empleo y funcionamiento del equipo material e inmaterial, tal y como se establece en el primer apartado. Esta regulación es insuficiente e incompleta, pues no tiene en cuenta los intereses en juego de las partes implicadas.

Por un lado, rompe, en parte, como ya lo hizo la Directiva, con la Ley Modelo sobre Firma Electrónica, que regula de forma completa los derechos y obligaciones de las partes que intervienen, haciendo un reparto de la responsabilidad entre todas ellas; por otro, como ya se dijo, pueden surgir problemas al establecer este tipo régimen de responsabilidad; pues, puede que los prestadores de servicios de certificación no quieran reconocer certificados extranjeros o claves expedidas por el grado de responsabilidad que asumen o pueden temer que la imposición de una responsabilidad y unas expectativa menores de diligencia, al prestador de servicios extranjero, limiten los recursos con los que puede contar en caso de falsificación o defraudación[907].

---

[905] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 53/2003, de Firma Electrónica,* Madrid, 2009, pág. 119.
[906] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica,* Madrid, 2009, pág. 105.
[907] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 86.

Como ya comentó el Prof. Madrid Parra[908], en referencia al Real Decreto-Ley sobre firma electrónica de 1999, resultan excesivas las obligaciones jurídico-privadas que son objeto de sanción administrativa y, así, no es aceptable que los proveedores de servicios estén absolutamente exentos de responsabilidad, pero tampoco resulta operativo y eficiente un régimen tan riguroso, que desincentive la actividad certificadora y, por ende, la seguridad en el comercio electrónico, proponiendo como vía de solución el diseño de un régimen de responsabilidad por la exclusiva actividad certificadora.

Esta crítica es predicable, igualmente, a la Ley de 2003, respecto al severo sistema de responsabilidad impuesto por la propia Ley; pues, junto a la responsabilidad civil se imponen sanciones de índole administrativa, que caminan, junto a las que imponen la norma sobre servicios de la sociedad de la información[909] (Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y del comercio electrónico), ya que al regularse de forma incompleta la responsabilidad, los prestadores de servicios de certificación estarán sujetos a esta norma.

Los servicios de certificación son servicios de la sociedad de la información, de acuerdo con la definición que de los mismos realiza la Directiva 98/48/CE[910]. Por ello, los proveedores de servicios que operen en España estarán sujetos, a la Directiva 2000/31/CE[911] dentro del ámbito normativo coordinado que ha de aplicarse a los mismos, y a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSICE). Si bien, la Ley de firma electrónica se aplica a todas las personas que generen y verifiquen firmas; es decir, a los prestadores de servicios de certificación y al no encontrar exclusión en las anteriores, cualquier vacío legal, existente en materia de responsabilidad en esta Ley, le será aplicable la Ley

[908] MADRID PARRA, A.: "Aspectos jurídicos de la identificación en el comercio electrónico" en *Derecho del comercio electrónico* (Dir. Illescas Ortiz, R.; coord. y Ramos Herranz, I.), Valencia, 2001, págs. 226 y ss.

[909] MÁRQUEZ LOBILLO, P.: "Prestación de servicios de certificación en la LFE", *Revista de contratación electrónica*, núm. 47, Marzo, 2004, pág. 29.

[910] Artículo 1,2-a) de la Directiva 98/48/CE del Parlamento Europeo y del Consejo, de 20 de Julio de 1998, que modifica la Directiva 98/34/CE por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas.

[911] Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

34/2002, creando aún más incertidumbre a los propio prestadores de servicios de certificación.

El legislador español, siguiendo al comunitario, aúna, bajo el mismo paraguas conceptual y jurídico, no solo las transacciones comerciales realizadas a través de redes de telecomunicaciones, sino también cualquier servicio que se demande y preste por tales vías electrónicas, con tal de que constituya una actividad económica para su prestador. Por ello, es forzoso reconocer que la LSSICE adquiere carácter de regulación general y supletoria para los prestadores de servicios de certificación, en defecto de normal especial, aportada por la Ley de firma electrónica Así, pues, le son aplicables a los mismo, materias contenidas en la LSSICE como: los principios de no sujeción a autorización previa, país de origen y libre prestación de servicios dentro del Espacio Económico Europeo, la obligación de comunicar al Registro Mercantil o Registro público correspondiente en el que deban estar inscritos, dominio o direcciones de Internet; asimismo, serían aplicables los deberes de colaboración y funcionamiento recogidos en la LSSICE; el régimen de responsabilidad, comunicaciones comerciales, contratación por vía electrónica, de infracciones, sanciones y de solución judicial y extrajudicial de conflictos[912]… todo ello, sin perjuicio de las eventuales especialidades que contemple la Ley de firma electrónica respecto a estas materias que, como norma especial, tienen una aplicación preferente.

6.1.4. Establecimiento de conducta y régimen de responsabilidad para el firmante y el prestador de servicios de certificación

6.1.4.1. China

La Ley recoge normas relativas a la responsabilidad de las partes: firmante y autoridad de certificación, centrándose, especialmente, en la autoridad de certificación; pues, aunque la Ley tiene una regulación general, pero extensa, en su Reglamento de desarrollo complementa y refuerzan las orientaciones que le son aplicables.

[912] COUTO CALVIÑO, R.: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista de la Contratación Electrónica*, núm. 83, Junio, 2007, pág. 4 – 37.

6.1.4.1.1. Firmante

El firmante debe proporcionar información verdadera, completa y precisa a la autoridad certificadora al solicitar el certificado y tener un cuidado razonable a la hora de proteger los datos; de manera que, si el firmante sabe que los datos de creación de firma pueden haber sido sustraídos o robados, debe notificarlo a la parte relacionada sin ninguna dilación y dejar de utilizar la firma (Artículos 15, 20 y 27).

Esta obligación se complementa con la obligación de la autoridad certificadora de comprobar la identidad del firmante, como información requerida en la expedición del certificado. De esta forma, el certificado electrónico debe contener obligatoriamente (Artículo 21): el nombre de la autoridad certificadora que lo emitió, el nombre del suscriptor, número de serie del certificado, fecha de validez y expiración, datos de validación, la firma electrónica de la entidad y cualquier otro elemento que el Ministerio pudiera determinar.

Por consiguiente, el firmante es responsable (Artículo 27) de los daños que pudieran sufrir las partes involucradas en el uso de la firma electrónica[913]: por no proporcionar información completa y veraz o en caso de que su firma electrónica haya sido sustraída o tenga indicios de que ha podido estar expuesta a algún tipo de peligro, en tanto en cuanto no lo haya comunicado en un tiempo razonable a las partes. Se recogen supuestos de responsabilidad del firmante por su eventual incumplimiento, que en algún caso podría ser de carácter penal, como es el supuesto contemplado en el Artículo 32, donde en el hecho de falsificar o usar de forma fraudulenta una firma electrónica, puede ser constitutivo de delito.

6.1.4.1.2. Autoridad certificadora

El servicio prestado por la autoridad de certificación es considerado como público, por lo que su regulación y, con ello, la intervención por parte del Gobierno se

[913] STEPHEN E. BLYTHE: "China's new electronic signature law and certification authority regulations: a catalyst for dramatic future growth of e-commerce", Chicago-Kent Journal of Intellectual Property, 2007, págs. 1 – 32.

considera justificada. Así, es el Ministerio de Industria y de la Información es la agencia gubernamental nacional designada: para otorgar licencias y regular la forma de otorgarlas[914]. Por ello, es criticable el minucioso control gubernamental, que contrasta con otras regulaciones, como es el caso de Estados Unidos o Singapur.

La Ley exige minuciosos deberes, que deben cumplir en el ejercicio de sus funciones, con el objeto de minimizar al máximo la posibilidad de cometer actos ilegales e, incluso, implícitamente podrían ir destinadas a la protección del consumir. Se observa un sistema de certificación obligatorio, de manera que nadie puede participar en las actividades de certificación a menos que el Ministerio lo haya autorizado mediante licencia. Para autorizar a la autoridad de certificación, ésta, previamente, debe cumplir una serie de requisitos: 1) que es una entidad jurídica autónoma; 2) tiene al menos 30 empleados; tiene un capital social de al menos al menos treinta millones de yuanes; 4) tiene un local de negocios físico apropiado, con un adecuado para el desarrollo de la actividad; 5) posee equipos y tecnología que cumplan los estándares de seguridad nacionales; y 6), demuestra que cumple con todas las leyes y reglamentos aplicables[915]. Al mismo tiempo puede revocar licencias si no mantienen el nivel de confianza e, incluso, promulgar disposiciones sobre la administración de servicios de certificación o supervisar a las autoridades proveedoras de servicios de certificación, de conformidad a lo previsto en la Ley (Artículo 25) [916].

Así, la autoridad certificadora, que pretenda participar en la emisión de certificados electrónicos en China, debe convencer al Ministerio de Industria de que utiliza un sistema fiable de emisión y revocación de certificados y, además, demostrar que cumple con las políticas generales, procedimientos y reglas previstas en la Ley y su reglamento de desarrollo.

Una vez que la autoridad de certificación ha obtenido la licencia por el Ministerio de Industria, debe registrarse como empresa comercial en un registro propiedad del

[914] KISSWAN, N. M.; AL-BAKR, A.: "Regulating the use of electronic signatures given the changing face of contracts", *MqJBL*, 2007, vol.7, págs.53-65.
[915] Artículo 17 del Certification Authority Regulations (Aprobado en el 12th Executive Meeting of the Ministry of Information Industry ("MII") de 28 de enero de 2005).
[916] STEPHEN E.; BLYTHE: "China's new electronic signature law and certification authority regulations: a catalyst for dramatic future growth of e-commerce", *Chicago-Kent Journal of Intellectual Property*, 2007, págs. 1 – 32.

Departamento de Comercio y publicar en su Web su número de licencia, así como cualquier otra información que determine el Ministerio (Artículo 18, in fine), recogidas en el Artículo 19, publicación de recomendaciones prácticas respecto al certificado electrónico expedido, reglas, código de prácticas de negocios, alcance de la responsabilidad, estándares operacionales, medidas de seguridad u otros asuntos relacionados con la actividad a realizar.

La Ley recoge tres tipos supuestos de responsabilidad para las autoridades de certificación con licencia[917]: a) establece que la autoridad certificadora será responsable cuando las partes sufran daños en el uso de la firma electrónica, en lo que respecta a las actividades basadas en los servicios de certificación proporcionados por el proveedor de servicios, salvo que demuestre la ausencia de culpa, lo que supone el establecimiento explícito de la carga de la prueba de una forma genérica (Artículo 28); b) una entidad emisora va a la quiebra sin informa al Ministerio con una antelación de sesenta días antes de declararse en quiebra, el Ministerio tiene el mandato de imponer una multa a la autoridad de certificación de 10.000 a 50.000 yuanes; y c) en el caso de no cumplir con las normas legales o cometa actividades ilegales., el director de la entidad será responsable directo.

Por otro lado, impone sanciones a las autoridades de certificación que ofrezcan sus servicios de certificación, sin licencia. En este supuesto el Ministerio ordenará el cese y confiscará las ganancias obtenidas (Artículo 29). Asimismo, se recoge la responsabilidad del personal del Ministerio de Industria, hasta tal punto que si no realizan las funciones encomendadas de forma correcta, se le impondrán las sanciones administrativas establecidas en el reglamento de desarrollo de la Ley, que podrán ser incluso de carácter penal (Artículo 33).

6.1.4.2. Singapur

Para entender el régimen de responsabilidad de las partes intervinientes en Singapur, debemos tener en cuenta la ratificación de la Convención de Naciones Unidas

[917] STEPHEN E. BLYTHE: "China's new electronic signature law and certification authority regulations: a catalyst for dramatic future growth of e-commerce", *Chicago-Kent Journal of Intellectual Property*, 2007, págs.1 – 32.

sobre Comunicaciones Electrónicas de 2005, que conllevó la modificación de la *Electronic Transaction Act*, en 2010.

Con este nuevo marco normativo se hace un planteamiento de la firma electrónica como un ingrediente vital en el éxito del comercio electrónico, siendo conscientes de que muchos de sus usos tienen lugar en transacciones no comerciales[918]. Su utilidad, en el ámbito del comercio, es lo que les ha dado el protagonismo que tienen internacionalmente en la actualidad. En muchos aspectos, tienen una estrecha relación con la tecnología digital; es decir, con la tecnología de cifrado, pero no son las únicas, ya que existen otros tipos mecanismos, que también están englobados en el concepto amplio de firma electrónica, que pueden utilizarse, actualmente, o cuya utilización futura puede estudiarse, con miras a cumplir una o más de las funciones de las firmas manuscritas.

Ante esto, se traza el principio de autonomía de la voluntad de las partes como eje de la Ley, con el fin de permitir a las partes suavizar, sin llegar al extremo, los requisitos legislativos sobre la firma, para propiciar métodos de autenticación, que ofrezcan un grado de fiabilidad a la firma electrónica. Para conseguirlo trata de no vincular la validez de una comunicación electrónica o de un contrato celebrado por medios electrónicos, a la utilización de una determinada firma electrónica[919].

Ya sabemos que uno de los desafíos de las firmas electrónicas se encuentra en una "definición" viable, aceptable y práctica que, a la vez, sea reconocida por todos los Tribunales de justicia. En la actualidad, no hay una "definición" de la firma electrónica internacionalmente acordada. Si nos preguntamos que entendemos por firma electrónica, se empieza por algo simple que al final, como en Europa, se va complicando, hasta llegar a la firma digital. A esta firma se le llena de términos, características y límites técnicos y jurídicos, que nos lleva a un problema de reconocimiento internacional, ante la falta de marcos comunes, porque al preguntarnos qué es la firma electrónica digital (o reconocida, segura, etc.) nadie puede responder,

[918] SENG, D.: "The Singapore Electronic Transactions Act and the Hong Kong Electronic Transactions Ordinance", *Digital Evidence and Electronic Signature Law Review*, núm. 5, octubre, 2008, págs. 7 – 20.
[919] CNUDMI/UNCITRAL: *Nota explicativa a de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, párr. 188.

únicamente, simplificando: es la firma equivalente a la firma manuscrita; pues, existen, respecto a esta pregunta, varias respuestas descoordinadas en los ordenamientos jurídicos nacionales.

De esta forma, las firmas electrónicas[920], y sus variaciones gramaticales, en Singapur, se entienden como los métodos electrónicos que se utilizan para identificar a una persona y para indicar la intención de esa persona, respeto de la información contenida en un registro; o sea, simplemente una confirmación de los usos o funciones de la firma electrónica (identidad, autenticación y autorización). Esta definición es, deliberadamente, lo suficientemente amplia, como lo era la Ley Modelo sobre Firma Electrónica[921], para abarcar todas las formas de identificación electrónica, desde la más informal e insegura, tales como las iniciales al final de un correo electrónico, a las muy formales y altamente seguras, como las biométricas (por ejemplo, las exploraciones de iris).

Se sabe que las firmas digitales son un subconjunto particular de la firma electrónica y es importante fijarlas, a la vez que resulta necesario argumentar su seguridad, con respecto a la responsabilidad de las autoridades de certificación, al ser la firma electrónica más utilizada, en el mismo sentido que la mencionada Ley Modelo, con el fin de facilitar la estipulación de mecanismos y productos para la responsabilidad, en el uso de las firmas digitales, evitando cualquier vacío legal que pudiera suscitarse. Este es el motivo por el que el legislador de Singapur decide regular este tipo de firmas, específicamente y conscientemente, en su Anexo segundo: para tratar todo lo referente a la firma electrónica digital, indicando la responsabilidad del firmante y del prestador de servicios de certificación, aunque sin establecer ninguna norma en materia de diligencia para la parte que confía.

[920] Singapur: Electronic Transactions Act 2010 (Cap. 88): "PART I: Interpretation 2. (1) In this Act, unless the context otherwise requires … "signed" or "signature" and its grammatical variations means a method used to identify a person and to indicate the intention of that person in respect of the information contained in a record".

[921] Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001): Artículo 2. Definiciones: "Para los fines de la presente Ley: a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos".

6.1.4.2.1. Firmante

En los Artículos 21 y siguientes se recogen las obligaciones del firmante, estableciendo un sistema basado en la diligencia, exponiendo sus grado, a través de un sistema escalonado con una norma general de diligencia razonable, como regla supletoria con respecto a las obligaciones del firmante que, sin embargo, pasa a ser una norma de garantía respecto de algunas obligaciones concretas, por lo general las relativas a la exactitud y veracidad de las declaraciones formuladas.

La Ley dispone que, al aceptar un certificado, el firmante certifica ante todos los que confían razonablemente, en la información contenida en dicho certificado, que: a) el suscriptor es el titular legítimo de la clave privada correspondiente a la clave pública señalada en el certificado; b) todas las declaraciones hechas por el suscriptor, a la autoridad certificadora y que sirvan de fundamento a la información consignada en el certificado, son veraces; y c) toda la información contenida en el certificado, que se halle en conocimiento del suscriptor, es veraz. A su vez, se prevé "la obligación de actuar con la debida diligencia para mantener el control de la clave privada, que corresponda a la clave pública consignada en dicho certificado, y prevenir su divulgación a toda persona no autorizada a crear la firma digital del suscriptor" (Artículo 24,1) [922].

6.1.4.2.2. Autoridad certificadora

En relación con la infraestructura de clave pública, en la que se basan las firmas digitales, sin la confianza de dónde reside la responsabilidad, los consumidores y las empresas no están dispuestos a asumir el uso de firmas digitales. Ésta es una cuestión tan importante como controvertida, tal y como estamos viendo.

La autoridad certificadora juega un papel importante, de tal manera que da fe de la identidad de los titulares de los certificados que emite. Las partes participantes en las transacciones en línea deben ser capaces de utilizar los certificados digitales, para

[922] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, pág. 86 y ss.

verificar de manera fiable la identidad de las partes en la transacción. Por ello, debido a su cargo de confianza, las autoridades de certificación deben ser sometidas a control.

El sistema de Singapur permite licencias voluntarias[923]; es decir, no requiere de otras autoridades de certificación para obtener una licencia, a diferencia de a lo regulado en la Directiva con su sistema de acreditación voluntaria. Sin embargo, impone una serie de requisitos, independientemente de si están autorizados o no, incluyendo la solidez financiera, la integridad de los datos recogidos, estrictos controles de seguridad y procedimientos. Estos requisitos incluyen que todas las autoridades de certificación deben emitir una declaración de prácticas de certificación o cumplir con los requisitos para la expedición de los certificados de digitales[924]; además, todas las autoridades de certificación deben cumplir con las normas legales, para la divulgación de información material sobre un certificado y los procedimientos involucrados en la revocación o suspensión de certificados (Artículo 27 y siguientes). El cumplimiento de estos requisitos los lleva a cabo el *Controller*[925], realizando auditorias de seguridad.

Si la autoridad certificadora obtiene la licencia podrá disfrutar de los beneficios de la presunción probatoria para las firmas digitales, generadas por el certificado que emita[926]. De esta manera, se le impone la obligación de verificar la exactitud de la información en que se basa para extender un certificado, si demuestra que ha cumplido con los requisitos establecidos en la Ley y el reglamento, puede condicionar esa garantía formulando la declaración correspondiente en el certificado, en el caso de no haber observado estas obligaciones, solo responderá hasta el límite de confianza especificado en el certificado[927].

---

[923] MASON, S.: *Electronic Signature in Law*, Cambridge, 2012, pág. 175.

[924] IDA: *Application form for accreditation / renewal of accreditation of certification authority* ("This application form is for Certification Authorities who desire to be accredited, or who desire to renew their accreditation, under the Electronic Transactions (Certification Authority) Regulations ("Regulations") made under the Electronic Transactions Act ("Act").").
Disponible en:
http://www.ida.gov.sg/~/media/Files/PCDG/Acts%20Regulations/ETA/ControllerCertAuthorities/CA_Accreditation_Renewal.pdf (última visita: 15/5/2014).

[925] ELECTRONIC TRANSACTIONS ACT 2010 (ACT 16 OF 2010): *Appointment of Controller*.
Disponible en:
http://www.ida.gov.sg/~/media/Files/PCDG/Acts%20Regulations/ETA/ControllerCertAuthorities/ApptOfControllerNotice.pdf (última visita: 15/5/2014).

[926] KAH LENG, T.: "Who bears the risk of mistake?", *Computer Law & Security Review*, septiembre - octubre, 2004, núm.20, vol. 5, págs.396–399.

[927] FEN LIM, Y.: "Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability", *Singapore Journal of International & Comparative Law*, 2003, págs.183–200.

El sistema de responsabilidad adoptado reconoce el derecho de la autoridad de certificación a expedir certificados de diferentes clases y de establecer diferentes niveles de confianza, a los que suelen corresponder diferentes niveles de limitación de la responsabilidad. Por ello, es destacable como Ley reconoce la importancia en el suministro de infraestructura de la información y del contenido, admitiendo un límite a la responsabilidad, que permite que se especifique en la declaración de prácticas de certificación y, en algunos casos, las exime de responsabilidad. Además, la autoridad certificadora acreditada podrá disfrutar de los beneficios de la presunción probatoria de las firmas digitales a los que certifica, lo que viene a suponer que la parte que confía en la firma, solo tiene que demostrar que la firma se ha verificado correctamente y, por tanto, la responsabilidad recaerá en la parte contratante que, en cualquier caso, deberá demostrar lo contrario[928].

En este contexto, se considera que no es práctico, para ellos, comprobar todos los contenidos a los que proporcionan acceso, por lo que se le indica que no estarán sujetos a responsabilidad civil o penal por material de terceros, en relación con los cuales no son más que un mero invitado. Sin embargo, esto no implica que no esté afecto a la responsabilidad en virtud de lo establecido en la Ley.

6.2. Planteamiento global: la responsabilidad en el uso de la tecnología de infraestructura de clave pública

Como dijimos anteriormente, la labor de la Ley Modelo no era abordar con detalle las cuestiones de responsabilidad, que pudieran corresponder a cada una de las partes intervinientes. Sin embargo, sí se apreció la importancia de que se fijaran unos criterios mínimos en relación, tanto con el firmante, como con el tercero que confía en el certificado y, evidentemente, el prestador de servicios de certificación. En esta estructura triangular se puede ver reflejada una específica ciencia o tecnología y de un concreto modelo de aplicación[929], en el establecimiento de infraestructuras de clave

[928] IDA SINGAPORE; ATTORMEY GENERAL'S CHAMBERS: *Joint IDA-AGC review of electronic, transactions act proposed amendments 2009*, LRRD No.1/2009, 30 de junio de 2009.
[929] MADRID PARRA, A.: "La identificación en el comercio electrónico", Revista de la Contratación Electrónica, Abril, 2001, págs. 3 - 60.

pública (ICP) u otras estrechamente relacionados con ésta. En este contexto, surgen cuestiones respecto a: la base jurídica que sustentaba los procesos de certificación, aplicabilidad del proceso de certificación, la asignación del riesgo y la responsabilidad de los usuarios, prestadores y terceros en el contexto del uso de técnicas de certificación, las cuestiones concretas de certificación, mediante el uso de registros y la incorporación por remisión, etc.[930]

Del estudio realizado se observa que las legislaciones de los distintos países, en torno a esta materia, plantean discusiones y dudas en torno a los distintos sistemas y tipos de responsabilidad, que se podrían exigir a las partes intervinientes en la transacción, especialmente, a las entidades de certificación en el ejercicio de su actividad. De esta manera, ante la posibilidad de que, a consecuencia de una prestación defectuosa del servicio de certificación, pudieran provocarse daños, bien a quienes hayan contratado dichos servicios o bien a terceros que se vean afectados por los mismos, siendo posible encontrar una serie de mecanismos, que establezcan los cauces apropiados, para permitir la reparación de los daños causados a las víctimas, estableciéndose como obligación del causante de dichos daños, reparar los mismos. De esta forma, se plantea una triple disyuntiva: la responsabilidad objetiva o subjetiva, la responsabilidad contractual o extracontractual y la responsabilidad limitada o ilimitada[931].

Asimismo, las ICP no se han prestado a la armonización a nivel internacional. Las ICP adoptadas, por los distintos Estados, comprenden cuestiones técnicas distintas, así como cuestiones de orden público, que dejan al arbitrio de cada Estado cuestiones que han sido abordadas a través de unas entidades "principales" de carácter público en la mayoría de los casos. Por consiguiente, se han adoptado cuestiones relativas a que tipos de entidades están dentro o pueden entrar en el sistema de ICP, a través del establecimiento de un proceso de autorizar a una entidad determinada, para actuar como entidad certificadora, debiendo tener una autorización expresa o licencia, por parte del Estado, o si debe utilizar otros métodos para controlar la calidad de las operaciones de

[930] CNUDMI/UNCITRAL: *A/CN.9/483 - Informe del grupo de trabajo sobre comercio electrónico acerca de la labor de su 37º período de* sesione, Viena, 25 de junio a 13 de julio de 2001, párr. 1 y ss.
[931] LAFUENTE SUÁREZ, M.: "La Ley de firma electrónica y la responsabilidad civil de los prestadores de servicios de certificación", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2007, núm. 13-1.

las entidades certificadoras[932]. Ante este panorama, podemos comprobar que el número de niveles de entidades, que se penetran en una ICP del Estado en cuestión, es casi nulo.

Además, se incluyen disposiciones en las Leyes relativas a qué entidades certificadoras son las adecuadas para emitir pares de claves criptográficas; si la validez de los pares de claves criptográficas deben ser entidades públicas o si también las entidades privadas podrían actuar como entidades certificadoras; el grado de seguridad, en el empleo de la técnica de criptografía, se debe autorizar; e incluso, si las autoridades gubernamentales deben poder tener acceso a la información codificada, mediante un mecanismo de supervisión en la custodia de claves.

Una forma de resolver algunos de estos problemas sería recurrir a uno o más terceros, para vincular a un firmante identificado o su nombre con una clave pública determinada[933], en referencia a cada una las funciones que pueden desarrollar las entidades de certificación, respecto a los pares de claves, que son: la función de emisor de la clave, la función de certificación y la función de confianza.

Sin embargo, la cuestión no se resuelve en este marco, si bien los prestadores de servicios pueden ser públicos o privados, la relación entre las diversas entidades certificadoras plantea cuestiones respecto al establecimiento de una estructura jerárquica, en la que algunas de ellas solo certifican a otras entidades certificadora. Así, las entidades certificadoras de una ICP pueden establecerse en una estructura jerárquica, en las que, algunas de ellas, solo certifican a otras entidades, que son las que prestan los servicios directamente a los usuarios, quedando dichas entidades certificadoras subordinadas unas a otras. En otras posibles estructuras pueden actuar en plano de igualdad; pero, en cualquier caso, si no existe una ICP internacional, pueden surgir problemas con respecto al reconocimiento de certificados por parte de entidades certificadoras de países extranjeros, ante la exigencia normativa en el cumplimiento de requisitos, que acarrean la responsabilidad de la entidad certificadora principal. Efectivamente, el reconocimiento de certificados extranjeros se puede realizar mediante la denominada "certificación cruzada"; sin embargo, cuando entran en juego diversas

[932] APEC: *Assessment Report on Paperless Trading of APEC Economies*, Pekín, 2005. Disponible en: http://publications.apec.org/publication-detail.php?pub_id=391 (última visita: 27/5/2014).
[933] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 36 y ss.

políticas de seguridad, plantean dificultades sobre la identificación del autor que generó el error, que causó una perdida, y de la fuente en que se basó el usuario[934].

A partir de lo anterior, la asignación de responsabilidad, en un marco de una ICP, se realiza de dos maneras: por medio de disposiciones contractuales o invocando normas de derecho; siempre, como eje, tendremos la figura del prestador de servicios de certificación, elemento típico en la relación tripartita, que es esencial en la infraestructura de clave pública, aunque no exclusivo de ésta. Por ello, la regulación del certificador es la que da origen a la mayoría de las normas específicas sobre firma electrónica. La necesidad de regulación específica en esta materia es diferente según se trate Derecho público o Derecho privado. Como es sabido, en el ámbito del Derecho Público es necesaria la norma expresa habilitante. En el Derecho Privado, por el contrario, rige el principio de la autonomía de la voluntad, no es necesaria una norma que autorice el uso de las nuevas tecnologías, ni siquiera la firma electrónica. Ahora bien, a efectos de seguridad jurídica, resulta conveniente una regulación[935]. En definitiva, lo que se trata es de regular la fuente de responsabilidad que se concreta con la actividad del prestador de servicios de certificación, que nos lleva a la responsabilidad frente a los daños derivados del uso de un certificado de identificación, que ha resultado adolecer de algún defecto en sí o en relación con la conducta del certificador.

En un principio, se presentaron dos cuestiones: la primera, referente a que una entidad nacional acreditara o garantizara los certificados extranjeros, dejándose apuntado que la primera asumiría la responsabilidad del certificado; la segunda, que los Estados regularán un régimen de reconocimiento de certificados extranjeros siguiendo criterios de reciprocidad[936]. Así, se suscitó la necesidad de especificar que dicha regulación se podría llevar a cabo mediante acuerdos bilaterales o multilaterales y,

---

934 CNUDMI/UNCITRAL: *Guía para la incorporación de la Ley Modelo de la CNUDMI para las Firmas Electrónicas al derecho interno,* Nueva York, 2001, párr. 58 y 59.

935 MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de la Contratación Electrónica*, abril, 2001, págs. 3-60.

936 COMISIÓN EUROPEA: *DICTAMEN DE LA COMISION con arreglo a la letra c) del apartado 2 del artículo 251 del Tratado CE, sobre las enmiendas del Parlamento Europeo a la posición común del Consejo sobre la Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO por la que se establece un marco comunitario para la firma electrónica POR EL QUE SE MODIFICA LA PROPUESTA DE LA COMISION con arreglo al apartado 2 del artículo 250 del Tratado CE (COM (1999) 626 final 1998/0191 - COD)*, Bruselas, 26 de noviembre de 1999, pág. 4.

además, se indicó que las entidades certificadoras podrían celebrar acuerdos generales de reconocimiento mutuo. Sin embargo, con posterioridad, se hizo constar la necesidad de acudir a un régimen flexible[937].

Las relaciones entre el firmante y el tercero dependerán de la naturaleza de las transacciones, en cualquier caso determinado. Por este motivo, en la mayoría de los ordenamientos jurídicos, el fundamento de la responsabilidad se ha fijado atendiendo a: a) el grado de culpa necesario para invocar la responsabilidad de una parte (grado de diligencia que una parte debe a la otra); b) las partes que pueden reclamar indemnización por daños y la magnitud de aquellos por los que puedan reclamarla; y c) si una parte culpable puede limitar su responsabilidad o exonerarse de ella y en la medida en que pueda hacerlo[938].

a) Grado de responsabilidad: en un marco de ICP la responsabilidad de las partes interesadas se basa en lo esencial en tres criterios posibles: la negligencia simple o culpa simple; la presunta negligencia (o culpa con inversión de la carga de la prueba); y la responsabilidad objetiva.

La negligencia simple es la adoptada por la Ley Modelo. El artículo 9,1 la recoge al hacer referencia a que un prestador de servicios apoye a una firma electrónica, "debe cerciorarse de todas las declaraciones importantes que haya hecho" (apartado b) y "debe proporcionar a la parte que confía en el certificado medios accesibles…" (apartado d). Toda persona está legalmente obligada a indemnizar a otra por las consecuencias negativas de sus actos.

En lo que atañe al firmante y a la parte que confía también se prevé la actuación conforme a una diligencia razonable de todo lo dispuesto en el Artículo 8 y en cuanto a la verificación de la firma o certificado respectivamente[939].

---

[937] MADRID PARRA, A.: Firmas digitales y entidades de certificación, a examen en la CNUDMI/UNCITRAL, *Revista de Actualidad Informática Aranzadi*., julio de 1997, núm. 24, págs. 3-31.

[938] CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 177 y ss.

[939] En varios países la ley va acompañada de una lista más o menos extensa de obligaciones positivas sin exponer el grado de diligencia previsto ni indicar las consecuencias del incumplimiento de esas obligaciones (Argentina). Sin embargo, en otros países la Ley complementa, expresamente, la lista de

Es decir, junto a la obligación genérica de actuar con diligencia, para evitar toda utilización no autorizada de la firma, se prevé la imposición al titular de las obligaciones de dar aviso, sin demora, de las actuaciones de riesgo de que la firma puede ser utilizada sin autorización y asegurar que son exactas y completas las declaraciones hechas por el titular de la firma a los certificadores de información y a las partes que confían en él[940].

La presunción de negligencia es el criterio adoptado en la Directiva 1999/93/CE y, posteriormente, en el Reglamento. El fundamento de este régimen es el supuesto de que, en determinadas circunstancias y en condiciones normales, los daños sólo pueden haberse producido, porque una parte no ha cumplido sus obligaciones o no ha observado una norma de conducta que había de respetar.

Se establece que el prestador de servicios de certificación es responsable del daño causado a cualquier entidad que confíe razonablemente en el certificado reconocido, salvo prueba de que no ha actuado con negligencia. La responsabilidad se basa en la negligencia con una inversión de la carga de la prueba, el prestador de servicios debe demostrar que no actuó con negligencia, ya que es quien mejor puede demostrarlo, por disponer de mejor técnica e información, algo que seguramente no tendrá ni el firmante ni el tercero que confía[941].

Con la responsabilidad objetiva[942] se trata de determinar si una persona es responsable simplemente por colocar en el mercado un producto defectuoso o por el mal funcionamiento de un aparato. Es una norma excepcional que no se suele presumir y que de momento parece que ningún país ha impuesto una responsabilidad objetiva ni al prestador de servicios de certificación ni a ninguna de las demás partes. No obstante, la responsabilidad del prestador de servicios tiene tintes de responsabilidad objetiva, pero estableciendo limitaciones a dicha responsabilidad.

---

obligaciones con una declaración general de responsabilidad del firmante por su eventual incumplimiento, que en un caso es incluso de carácter penal (México).

940 DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 459.

941 El Art. 6 de la Directiva 1999/93/ CE, se establece un grado de responsabilidad al prestador de servicios de certificación que podría ser aumentado por los Estados.

942 BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, 2004, núm.3, vol. 4, págs.211-242.

Como ha comentado la Prof. Martínez Nadal, el legislador español y el comunitario han obviado otros supuestos de responsabilidad derivados de la revocación, como la responsabilidad por posibles utilizaciones ilegítimas de la clave de firma, desde el momento de la pérdida de la misma hasta la publicación de la revocación del certificado correspondiente. A falta de criterio legal expreso, como ocurre en el caso de pérdida de tarjetas de crédito y la clave correspondiente, acabará asumiendo esta responsabilidad el titular del certificado; pero en ambos casos sería deseable la existencia de límites a tal responsabilidad, especialmente rigurosa, pues puede llegar a ser objetiva, independientemente de la diligencia o negligencia del titular en la custodia de la clave[943].

Asimismo, en el tráfico contractual, el importante volumen de las operaciones, y las especiales características de los medios empleados, esta opción también encuentra la dificultad de que, a veces, se llegaría a la imposibilidad de acreditación de la diligencia debida; es decir, a una prueba negativa por parte del prestador de servicios de certificación, auténtica *probatio diabólica*, y supondría, en la práctica, la imposición de una responsabilidad objetiva e ilimitada; pues, siempre va a ser más fácil demostrar que no se ha actuado con negligencia, en la medida en que se pruebe que se ha actuado con un mínimo de diligencia, que probar que se ha actuado con la diligencia, que cabría esperar del prestador[944].

No obstante, la Directiva, en el apartado tercero del Artículo 6, y el Reglamento en su Artículo 24,2-c), y, por tanto, los Estados miembros, recogen un margen permitido para que el proveedor de servicios pueda limitar el grado de responsabilidad que le es exigible. Se refiere ese ámbito a la limitación de los posibles usos del certificado reconocido, así como al valor límite de las transacciones que puedan realizarse con el mismo, en base al conocimiento subjetivo del límite en cuestión.

El tercero que confía debe tener conocimiento de la existencia del mencionado límite, debiendo el prestador de servicios establecer un sistema técnico que no permita su superación y que avise fehacientemente sobre los límites de uso del certificado; como

[943] MARTÍNEZ NADAL, A.: *Comentarios a la Ley 59/2003, de firma electrónica*, Madrid, 2009, págs.
[944] ERDOZÁIN LÓPEZ, J. C.: "Firma electrónica, aspectos procesales, valor probatorio modelos de responsabilidad de los prestadores de servicios de certificación", Revista Aranzadi Civil, abril, 2003.

consecuencia, el proveedor de servicios de certificación no será responsable por los perjuicios que pudieran derivarse de la superación del límite máximo de un certificado reconocido, indicado en el mismo o bien por el exceso en el uso del certificado.

De esta manera, se deja claro con esta disposición que un proveedor de servicios de certificación no es responsable del uso abusivo del certificado[945]. Así, en España, se considera que cuando los niveles de seguridad y las políticas se pongan en conocimientos de los usuarios y no haya negligencia por parte de la entidad certificadora, habrá un desplazamiento de la responsabilidad[946].

b) Las partes con derecho a reclamar daños y perjuicios y alcance de los daños y perjuicios exigibles[947]: La responsabilidad contractual suele derivarse del incumplimiento de una obligación contractual. En un contexto de ICP, generalmente, existe un contrato entre el firmante y el prestador de servicios de certificación. Las consecuencias del incumplimiento de las obligaciones contractuales de uno frente al otro se determinan por el propio texto del contrato.

En esta cuestión es obligada la referencia al apartado 5 del Artículo 12 de la Ley Modelo sobre Firma Electrónica, que prevé el acuerdo entre las partes como suficiente para el reconocimiento transfronterizo de una firma electrónica, siendo importante para ello, dar efecto a las estipulaciones contractuales conforme a las cuales, podrán convenir dicho reconocimiento en el uso de firma electrónicas o certificados, recurriendo a la autonomía de las partes como motivo suficiente para el reconocimiento transfronterizo. Esta norma repite el principio de autonomía de la voluntad del Artículo 5 de la Ley Modelo, lo hace refiriéndose a que siempre es posible que las partes pacten entre sí el

[945] COMISIÓN EUROPEA: *DICTAMEN DE LA COMISION con arreglo a la letra c) del apartado 2 del artículo 251 del Tratado CE, sobre las enmiendas del Parlamento Europeo a la posición común del Consejo sobre la Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO por la que se establece un marco comunitario para la firma electrónica POR EL QUE SE MODIFICA LA PROPUESTA DE LA COMISION con arreglo al apartado 2 del artículo 250 del Tratado CE (COM (1999) 626 final 1998/0191 - COD)*, Bruselas, 26 de noviembre de 1999, pág. 4.

[946] Véase Artículo 23, 4 y 5 de la Ley 59/2009, 19 de Diciembre, de firma electrónica sobre "Limitaciones de la Responsabilidad de los prestadores de servicios de certificación".

[947] CNUDMI/UNCITRL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 194 y ss.

reconocimiento de determinados certificados o firmas electrónicas reuniendo la validez que establezca el Derecho aplicable para cada acuerdo[948].

En el caso de las firmas y los certificados electrónicos puede haber responsabilidad más allá de una relación contractual claramente definida; pues, el tercero que confía no celebra un contrato con el prestador de servicios de certificación, y, además, no tiene relación alguna con él; solo confía en el certificado. Ello puede plantear cuestiones difíciles, que algunos ordenamientos no han acabado de resolver. Nos referimos al hecho que han recogido las legislaciones, por ejemplo, en lo referente a la inexactitud en los datos contenidos en un certificado o la no incorporación al mismo de datos que debieran figurar, que pueden llegar a daños tanto al titular del certificado, que podría perder oportunidades de negocio, como a terceros que hayan confiado en dicho certificado. Cabe señalar, países como Singapur, donde las normas jurídicas, cuando los niveles de seguridad y las políticas, se pongan en conocimiento de los usuarios, mediante la emisión de una declaración de prácticas de certificación y no haya negligencia, por parte de las entidades certificadoras, no habrá responsabilidad.

Este hecho se produce en el momento de realizar la operación contractual que se suscribe con la firma electrónica. Las entidades de certificación no intervienen en forma alguna, por lo que, en consecuencia, tampoco disponen de posibilidad de autorizar o no la operación que se va realiza. Esta imposibilidad de veto, a la consecución de una operación contractual, hace que la responsabilidad a que se enfrentan los prestadores de servicios de certificación pudiera llegar a ser indefinida e ilimitada, por lo que en la práctica dicha circunstancia haría que se produjese una proliferación de cláusulas limitativas y exonerativas de responsabilidad que, además de poder resultar abusivas, por su contenido, podrían ir contra la misma función y utilidad del certificado[949]. Sin embargo, en este contexto parece importante la necesidad de establecer un sistema objetivista a este respecto, pero sin olvidar los sistemas de imputación de responsabilidad por culpa; pues, como dijo nuestro Tribunal Supremo "la exigencia del elemento culpabilístico y acrecentada la correlativa tendencia objetivadora de esta clase de responsabilidad, siempre será requisito ineludible la exigencia de una relación de

[948] MADRID PARRA, A: Ley Modelo de la CNUDMI/UNCITRAL para las firmas electrónicas, *Revista derecho patrimonial*, Año 2003 – 2, núm. 11, pág.59.
[949] LAFUENTE SUÁREZ, M.: "La Ley de firma electrónica y la responsabilidad civil de los prestadores de servicios de certificación", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2007, núm. 13-1.

causalidad entre la conducta activa o pasiva (acción u omisión) del demandado y el resultado dañoso producido"[950].

c) Capacidad de limitar contractualmente la responsabilidad o renunciar a ella[951]: durante la preparación de la Ley Modelo se convino que, en los casos en que un prestador de servicios de certificación trabajara con arreglo al derecho de un Estado extranjero, debían evaluarse las posibles limitaciones de la responsabilidad del prestador de servicios de certificación, mediante una referencia al derecho de ese Estado extranjero[952]. De esta forma, deberían tenerse en cuenta las normas que rijan la limitación de la responsabilidad en el Estado en que esté establecido el prestador de servicios de certificación o en cualquier otro Estado, cuya legislación sea aplicable en virtud de las reglas pertinentes sobre conflictos de leyes. De esta forma, al evaluarse la responsabilidad del prestador de servicios de certificación, deberían tenerse en cuenta una serie de factores: 1) el costo de obtención del certificado; 2) la naturaleza de la información que se certifique; 3) la existencia de limitaciones de los fines para los que pueda utilizarse el certificado y el alcance de esas limitaciones; 4) la existencia de declaraciones que limiten el alcance o la magnitud de la responsabilidad del prestador de servicios de certificación; y 5) toda conducta de la parte que confía en la firma que contribuya a la responsabilidad[953].

Las cláusulas de limitación de responsabilidad es algo que suele encontrarse en la documentación de un contrato. Por ello, la Directiva, y en le mismo sentido el Reglamento de la UE, no establece un tope en la responsabilidad en la que puede incurrir, pero si le permite indicar un valor máximo, por operación, para cada certificado (Artículo 6 de la Directiva, Artículo 24,2). Sin embargo, la limitación por responsabilidad la establecen los Estados miembros, en el caso español en el Artículo 23 de la Ley 59/2003.

[950] Sentencia del Tribunal Supremo (Sala de lo Civil) núm. 677/1994, de 9 julio (RJ 1994\6302).
[951] CNUDMI/UNCITRL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, párr. 202 y ss.
[952] CNUDMI/UNCITRAL: *A/CN.9/484 - Informe del Grupo de Trabajo sobre Comercio Electrónico acerca de 38º período de sesiones*, Nueva York, 12 a 23 de marzo de 2001, párr. 74 y ss.
[953] CNUDMI/UNCITRAL: *Guía para la incorporación de la Ley Modelo de la CNUDMI para las Firmas Electrónicas al derecho interno*, Nueva York, 2001, párr.146 y ss.

La obligación básica de los prestadores de servicios de certificación; no es otra, que la de "utilizar sistemas, procedimientos y recursos humanos fiables y actuar de conformidad con las declaraciones que hagan respecto de sus normas y prácticas". Por ello, se les presupone una actuación con diligencia razonable, como ya se ha comentado, en el ámbito de la Ley Modelo, que les lleva a cerciorarse de todas las declaraciones hechas, en relación con un certificado o firma electrónica, sean exactas.

Todo ello puede generar diversos grados de responsabilidad, según el Derecho aplicable:

- Cuando no se expide un certificado o se demora en expedirlo, es posible que un solicitante cumpla los requisitos establecido por el prestador de servicios de certificación y que su solicitud sea rechazada o aplazada, bien por un error, bien por otros motivos desea retrasar o denegar la expedición del certificado. En tales circunstancias, el solicitante podrá demandar al prestador de servicios. El nacimiento a cargo del prestador de servicios de certificación de esta obligación viene del resarcimiento a los usuarios, que hayan confiado en el contenido del certificado, en requerimiento de la buena fe de éstos[954].

- Uso de la firma sin autorización o validez cuestionable, reviste dos aspectos: por una parte, es posible que el dispositivo de creación de firma no esté debidamente protegido o que su seguridad se vea comprometida de otra manera (por ejemplo, por apropiación indebida). En cambio la jerarquía del propio prestador de servicios de certificación, con respecto a la firma, puede quedar en entredicho si su clave de firma se pierde, se divulga o es utilizada por otras personas sin autorización o si se ve comprometida de alguna otra manera. Esta cuestión no se plantea en la Ley Modelo sobre Firma Electrónica; sin embargo, cabe presumir la obligación general del prestador

[954] Observemos, cómo la Ley Modelo, en su Artículo 4 apartado 1, nos dice: "En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe". De esta forma, se trata de advertir a la persona que deba aplicar la Ley Modelo de que las disposiciones de éste (o las disposiciones del instrumento por el que se dé aplicación a la Ley Modelo), aunque estén incorporadas a la legislación nacional y sean por tanto derecho nacional, deben interpretarse teniendo en cuenta su origen internacional, a fin de asegurar la uniformidad en la interpretación de la Ley Modelo en todos los países promulgantes.

de servicios de certificados prevista en la citada Ley Modelo, en cuanto a "utilizar sistemas, procedimientos y recursos humanos fiables", que abarca el deber de adoptar todas las medidas que sean necesarias para impedir que su clave quede en entredicho. La seguridad del sistema de certificados emitido por el prestador de servicios se halla respaldada a su vez por la firma electrónica de éste, que se adjunta al certificado, permitiendo corroborar, al tercero que confía en el certificado, si los contenidos en el certificado han sido o no alterados[955], acercando la responsabilidad a la figura de la entidad certificadora. Por ello, se impone en la mayoría de los ordenamientos, aunque con algunas variaciones, la exigencia al firmante de que "actué con diligencia razonable para evitar la utilización no autorizadas de sus datos de creación de la firma".

- Cuando se actúa con negligencia al extender un certificado, sería el supuesto, por ejemplo, de usurpación de identidad del firmante; es decir, la función principal de una firma o certificado electrónico es la de identificar al firmante; la función principal del prestador de servicios es la de "cerciorarse de todas las declaraciones importantes hechas en relación con el ciclo vital del certificado o que estén consignadas en él, sean exactas y cabales" (Artículo 9,1-b) de la Ley Modelo sobre firma electrónica), de lo contrario responderá frente al firmante y al tercero de confianza por el perjuicio que pudiera causar su error. Esta obligación la podemos encontrar en el Artículo 6,1 de la Directiva 1999/93/CE, Artículo 24,1 del Reglamento y Artículo 12 Ley 59/2003 de firma electrónica, que impone exigencias mayores a la pura "diligencia razonable" impuesta por la Ley Modelo. Esta obligación tiene su complemento en la obligación del firmante de "actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma" (Artículo 8,1-a) de la Ley Modelo sobre Firma Electrónica) por la que recaerá, en la figura del firmante, la responsabilidad frente al tercero en confianza e incluso frente al prestador de servicios. En cualquier caso, la responsabilidad se asemeja a las anteriores en la medida de que afecta la veracidad de los certificados.

[955] LAFUENTE SUÁREZ, M.: "La Ley de firma electrónica y la responsabilidad civil de los prestadores de servicios de certificación", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2007, núm. 13-1.

- El hecho de no suspender o no revocar un certificado, el prestador de servicios de certificación podría incurrir en responsabilidad por no suspender o revocar un certificado de validez cuestionable, ya sea por el uso de la firma sin autorización, ya por uso de forma indebida de la misma, ya por lo que podría ser una apropiación indebida. Casos en los que toda seguridad jurídica de cualquier individuo está en entredicho, la rapidez con la que se actúe es vital para todo tercero que confía y por supuesto para el firmante. Así, la figura del fraude está latente y, por ello, la Ley Modelo exige al prestador de servicios de certificación que proporcione, a la parte que confía en el certificado, "medios razonablemente accesibles que permitan determinar mediante el certificado si existe un medio para que el firmante de aviso de que los datos de creación de la firma están en entredicho o si ofrece un servicio para revocar oportunamente el certificado" (Artículo 9,1 d-v y vi de la Ley Modelo)[956].

  Obligación análoga es impuesta al firmante en el Artículo 8 de la Ley Modelo pues "sin dilación indebida utilice los medio que le proporcione el prestador de servicios de certificación o en cualquier caso esforzarse razonablemente para dar aviso a cualquier persona que según pueda prever el firmante… que la firma ha podido quedar en entredicho o las circunstancias dan lugar a un riesgo considerable de que los datos de la firma han quedado en entredicho".

6.3. La pretendida libre competencia

La situación que se presenta, para que las entidades que prestan servicios de firma electrónica puedan actuar en el mercado, como todo lo que se refiere a Internet y al comercio electrónico, es deudora de las posturas que se han adoptado en la práctica. Antes de que los Estados lanzasen su normativa sobre firma electrónica, está ya existía. La postura práctica, para el desarrollo del comercio electrónico, había sido auspiciada por las grandes empresas y la banca, interesadas en el desarrollo del comercio

[956] Misma obligación impuesta en la Directiva 1999/93/CE, Art. 6,2 y apartado b) del Anexo II.

electrónico y de los servicios financieros, en un entorno telemáticos, al margen de cualquier control gubernativo.

La dimensión mundial del comercio electrónico ha demandado certidumbre jurídica en el uso de las nuevas tecnologías. Con el fin de que poder llevar a cabo, responsablemente, los negocios en línea, los usuarios deben asegurarse de que cada transacción electrónica es legalmente vinculante y ejecutable[957]. Así, por un lado, en el mundo real, las personas que usan un pasaporte o documento de identificación, para identificarse en cualquier negocio jurídico que realizan; por otro, en el mundo electrónico, en el uso de la tecnología digital, un usuario puede proporcionar su identificación con un certificado electrónico y crear una firma electrónica legalmente vinculante, en forma de correo electrónico o la web. El receptor puede luego validar la identidad del usuario con ese certificado y tener la certeza de que el mensaje no ha sido alterado.

En el establecimiento de métodos de firma y autenticación electrónica fiables, es importante identificar a los sujetos que participan en el tráfico jurídico electrónico, que son portadores de derechos y obligaciones, sujetos que, de una forma expresa o implícita, son identificables en todas legislaciones. Como sabemos, la figura sobre la que descansa el sistema de firma electrónica es la del prestador de servicios de certificación; esto es, son los prestadores de servicios de certificación los que mantienen el sistema y asumen la responsabilidad de su buen funcionamiento, constituyéndose en garantes de la seguridad[958], especialmente, en los Estados que establecen el empleo de las técnicas de criptografía de clave pública.

Su intervención es necesaria, como ilustra el empleo de estas técnicas, para garantizar la asociación entre un par de claves y una persona determinada, así como para una distribución efectiva de las claves. Sobre la base del certificado expedido y firmado por aquél, se garantiza frente a terceros su integridad y origen[959]. Sobre la base de la autonomía de la voluntad que rige en el sector privado, se expande el uso de la

[957] MADRID PARRA, A.: "Contratos electrónicos y contratos informáticos", Revista de la Contratación Electrónica, enero, 2011, núm.111, págs. 5 – 35.
[958] COUTO CALVIÑO, R: *Servicios de Certificación de Firma Electrónica y Libre Competencia*, 2008, Madrid, págs. 58 y ss.
[959] DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002, pág. 312 y ss.

identificación por medios electrónicos. A lo más, se aplican normas de origen convencional. Y desde luego, la identificación, mediante firma electrónica, sobre la base de la infraestructura de doble clave, se articula en torno a la intervención de sujetos privados sin participación de ente público alguno. La necesaria intervención de terceros, que certifican la identidad de quienes plasman una firma electrónica, no descansa sobre los atributos legales conferidos a la fe pública, sino sobre el crédito adquirido por quienes en el desarrollo de los negocios se ganan la confianza de los demás. Así, las llamadas autoridades de certificación, que nacen en Estados Unidos, para certificar la identidad de los titulares de firmas electrónicas, no son autoridades en el sentido de poder público, sino empresas cualificadas en el sentido de conocimiento del negocio que certifican o acreditan la identidad de terceros, que utilizan la firma electrónica, si bien con desigual grado o nivel de garantía de la certificación, según los casos[960].

Visto lo anterior, nos encontramos ante el hecho de que las entidades privadas comenzaron a operar sin que hubiera regulación alguna. Esto llevo a la CNUDMI[961], en sus Leyes Modelos, a evitar ir al establecimiento de un modelo de licencia o limitador del uso de las nuevas tecnologías, que pudiera provocar el establecimiento de barreras que crearan problemas difíciles de solucionar. Este camino fue seguido, en un principio, por las legislaciones estatales. Sin embargo, todas han establecido algún tipo de control que, en mayor o menor medida, impide el establecimiento de los principios que fueron marcados en las Leyes Modelos por la CNUDMI.

De esta forma, como hemos visto, muchos han sido los Estado que han establecido un marco técnico-jurídico para autenticación electrónica que les permite, en principio, operar[962]. Un esquema puede incluir: por un lado, el establecimiento de estándares nacionales e internacional de productos y servicios relacionados con la autenticación electrónica; y por otro, la creación de un marco para regular la supervisión, la acreditación y la certificación de algunos o todos los productos y servicios de autenticación. Cuando dicho marco está en su lugar, puede ser que se

[960] MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de la Contratación Electrónica*, Abril, 2001, págs. 3 – 60.
[961] CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE* (2001), párr. 118.
[962] BLANCHETTE, J.L.: "Defining Electronic Authenticity: An Interdisciplinary Journey", *Conferencia internacional sobre sistemas y redes fiables*, Florencia, 28 de junio-1 de julio, 2004.
Disponible en: http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (última visita: 27/5/2014).

establezca por el Estado o por un sistema voluntario de acreditación, que establezca, en principio, directrices, mejores prácticas u otras cuestiones relacionadas con la prestación de infraestructuras de autenticación[963].

Este último supuesto es el punto en el que nos centraremos; pues, es aquí donde nos encontramos ante una serie de controles que se centran en el control de la actividad del prestador de servicios de certificación. De esta forma, estamos ante una serie de controles que vienen a fijar un sistema de autenticación de certificados nacional, en pro de un establecimiento de una mayor seguridad, con el fin de conseguir una mayor confianza del usuario final.

Estos controles de cara a dar seguridad al sistema vienen a realizarse, en la mayoría de las legislaciones, por una autoridad pública. Y se establecen de distintas maneras; en Estados Unidos se realiza, como hemos dicho a través del establecimiento de disposiciones relativas a la defensa de los consumidores; Singapur, trata de establecer un marco jurídico y normativo propicio para crear un ambiente de confianza, previsibilidad y certidumbre para que el comercio electrónico prospere, con la ratificación de la Convención de Naciones Unidas. Por ello, establece un sistema de licencias voluntario de las autoridades de certificación, con objeto de promover la acreditación de estas entidades, estableciendo requisitos estrictos de integridad y seguridad. De esta forma, establece en el Artículo 27 de su Ley, que toda las entidades emisoras de certificados y registros serán examinadas por una entidad, antes de que el prestador de servicios pueda obtener la acreditación como entidad de certificación, denominada *Controller*, designada por el Ministro, pudiendo éste nombrar a cualquier persona para que sea el controlador para los fines de la Ley. Otro sistema es el adoptado en China, donde el sistema de certificación resulta obligatorio, de manera que nadie puede participar en las actividades de certificación, salvo que se encuentre autorizado para ello.

En Europa, por un lado es un sistema obligatorio respecto de terceros países; y por otro, un sistema de acreditación voluntaria, tal y como se puede observar en la Directiva 1999/93/CE sobre firma electrónica y el Reglamento, en el establecimiento de la libre

[963] MASON, S.: *Electronic Signature in Law*, Cambridge, 2012, págs.174 y ss.

prestación de estos servicios en el ámbito de la Unión Europea, partiendo así de los mismos principios que estableció la CNUDMI en su Ley Modelo sobre Firma Electrónica. Sin embargo, como hemos dicho anteriormente, a pesar de la proclamación de esta libre prestación de servicios de certificación de firma electrónica, cuando los certificados sean reconocidos cada Estado miembro, éstos tienen la última palabra, no de autorizar sino de dar la conformidad a los productos a nivel interno. Asimismo, el Estado puede establecer prescripciones adicionales para el uso de la firma electrónica en el sector de público.

Por esto, podemos decir que a la luz del régimen establecido por el legislador comunitario se está dando a los Estados miembros la posibilidad de establecer barreras para el acceso y el libre desarrollo de la actividad. La forma de hacerlo ha sido a través de recoger, en las legislaciones, nuevos requisitos, añadidos a los recogidos en la propia Directiva y, además, se otorga la posibilidad de que un prestadores de servicios de certificación, de naturaleza pública, pueda realizar actividades de certificación, como si de una entidad privada se tratara, comprometiéndose de manera directa la libre competencia.

Alemania, en la SigG, establece la libre circulación de firmas cualificadas en el ámbito de la Unión Europea. Sin embargo, señala que el funcionamiento de los prestadores de servicios de certificación cumplirán los requisitos de seguridad, fiabilidad y solvencia técnica y económica. Sin embargo, con la realización de la "Declaración jurídico-privada para promover el uso de firmas digitales", se aprecia una mejor forma de fomentar la libre competencia.

Italia, en su Decreto Legislativo 82/2005, establece que la prestación de los servicios de certificación es libre y no necesita autorización previa, pero deben cumplir unos requisitos de honorabilidad. Estos requisitos de honorabilidad son mismo que se les exigen a los directivos bancarios, teniendo en cuenta que el Banco Central de Italia actúa, junto a la CNIPA, como vigilantes del cumplimiento de los requisitos de certificación de firma digital.

España, la prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer

restricciones para los servicios de certificación, que procedan de alguno de los Estados miembros de la Unión Europea, aunque en la formulación del principio, por parte del legislador español, se constata una opción restrictiva: la libre competencia se predica solo para los proveedores de la Unión Europea.

Asimismo, se presencia una quiebra real de la libre competencia en el mercado español, teniendo en cuenta la situación de monopolio que ejerce la Fábrica Nacional de Moneda y Timbre (FNMT) debido, no sólo a la gratuidad de sus certificados, sino también por la exclusividad de la que goza hasta hace unos años. La FNMT presta servicios a particulares y a entidades privadas, que nada tienen que ver con la Administración, tales como los propios del tráfico de empresas privadas como las citadas en su página web[964]. Así pues, la FNMT se configura como un prestador de servicios de certificación en régimen de competencia, que expide certificados de firma electrónica, que puede desempeñar otras funciones, siempre relacionadas con ella; es decir, la FNMT desarrolla sus competencias en el ámbito de la seguridad e integridad de las comunicaciones electrónicas, garantizando con su intervención la procedencia de quién envía el documento electrónico, la integridad del contenido del documento y su confidencialidad. Es este su concreto campo de actuación, tal cual resulta de la propia Directiva 99/93/CE[965].

Además, han proliferado entidades de certificación vinculadas con la Administración, o integrantes de lo que se denomina órganos de Administración corporativa, tales como las sociedades CAMERFIRMA[966], participada por el Consejo General de Comercio, Industria y Navegación de España, o ANCERT[967], constituida por el Consejo General del Notariado de España, que ofrecen sus servicios a particulares con una finalidad netamente comercial.

Con el Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, la situación cambia

[964] Fábrica Nacional de Moneda y Timbre (FNMT).
Disponible: http://www.cert.fnmt.es/index.php?o=cert (última vista: 27/5/2014).
[965] Sentencia del Tribunal Supremo de 2 de julio de 2001 (RJ 2001\5397).
[966] CAMERFIRMA.
Disponible en: http://www.camerfirma.com/ (última vista: 27/5/2014).
[967] ANCERT.
Disponible en: www.ancert.com (última vista: 27/5/2014).

respecto a la libre circulación de prestadores de servicios de certificación en ámbito europeo, que en su Artículo 4 determina los principios del mercado interior en lo que se refiere a la aplicación territorial del Reglamento. Se hace mención explícita de que no se impone ninguna restricción a la libre prestación de servicios ni a la libre circulación de productos; aunque si observamos que considera (Considerando 12 y 13) que los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de autenticación o identificación electrónica, medios de acceder a los servicios en línea, aunque no se impondrá restricción alguna a la prestación de servicios de confianza, en el territorio de un Estado miembro, a un proveedor de servicios de confianza establecido en otro Estado miembro, por razones que entren en los ámbitos cubiertos por este Reglamento, y que se permitirá la circulación libre y segura en el mercado interior de los productos que se ajusten al presente Reglamento. Habrá que estar a lo que se los beneficios o a los que se puedan beneficiar de un conjunto común de requisitos de seguridad para los servicios de confianza, que se podrán establecer, ante la introducción de los distintos niveles de seguridad, y, por tanto, de un nivel de seguridad mínimo, como requisito previo necesario para el principio de reconocimiento mutuo y, que si bien contribuirá a aumentar el nivel de seguridad en el entorno digital, también puede contribuir a restringir el reconocimiento.

6.4. Gestión de la responsabilidad

6.4.1. Planteamiento

El comercio electrónico y la firma electrónica no se circunscriben sólo al ámbito nacional, encontrándonos una necesidad de reconocimiento jurídico de ámbito internacional. Contractualmente, las partes podrían incluir una cláusula de elección expresa de la Ley aplicable, bajo el principio de autonomía de la voluntad de las partes.

Sin embargo, cuando no existe este pacto expreso o implícito, el contrato se regirá por la Ley de la jurisdicción que tenga los vínculos más estrechos con el contrato[968].

[968] DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009, pág.183 y ss.

Esto puede depender, especialmente, de la materia, la nacionalidad o el domicilio de las partes, el lugar de celebración, lugar de ejecución, etc.[969].

El elemento extranjero, en una situación jurídica, complica la respuesta práctica a la misma, sea judicial o extrajudicial, por concurrir en él distintos intereses y por hallarse vinculada con diferentes ordenamientos jurídicos. La mayoría de los sistemas jurídicos se basan en el principio de que los Estados soberanos ejercen jurisdicción exclusiva dentro de su propio territorio. Este principio se refleja en el de Derecho internacional público, por el que cada Estado tiene jurisdicción para emitir y aplicar sus propias leyes dentro de sus límites territoriales[970].

Ante esta situación podemos encontrarnos, a la hora de determinar el Derecho aplicable o las reglas de ese sistema de Leyes que se aplican al contrato, con varios supuestos:

- Si todas las partes se encuentren físicamente ubicadas en un mismo Estado, será fácil la determinación de la Ley aplicable; por ejemplo, si todas las partes se encontraran en territorio español.

- Si una de las partes litigiosas reside en España y la otra es una persona física o jurídica autorizada para hacer negocios en España; es decir, un prestador de servicios de certificación que cumple con los requisitos establecidos en la Ley, tenga su sede o no su sede en España, también será, más o menos fácil, asumir la jurisdicción aplicable.

- Por el contrario, la situación se complica cuando el demandado no es ni residente español ni una persona jurídica autorizada a realizar negocios por la legislación del Estado del foro, porque la persona física o jurídica no se encuentra físicamente dentro de España o no tiene permiso expreso para hacer

[969] Artículos 2 y siguientes del Reglamento 44/2001, del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (D.O.U.E. serie L, núm. 12, de 16 de enero).
[970] INTVEN, H.; PFOHL, R.; SLUSARCHUK, C.: "Legal and regulatory aspects of e-commerce and the internet", *The World Bank Legal Review. Law and Justice for Development*, núm.1, 2003, págs.3-160.

negocios en dicho foro y, por tanto, los Tribunales estatales carecen de jurisdicción; o puede ser que, la persona física o jurídica española, que tenga un conflicto de intereses en relación con un contrato firmado electrónicamente, con una persona de un tercer país, donde sí se reconoce efectos jurídicos a la firma del empresario español y, por tanto, el contrato es válido, tendrá necesariamente que litigar fuera de España, porque aquí no puede exigir el cumplimiento del contrato al no reconocerse la firma electrónica del empresario extranjero. Ante esto, nos encontramos con el interrogante de la extraterritorialidad de la jurisdicción y, desde que punto de vista, debemos encontrar una solución. Hablamos de sí en un foro se me permite hacer algo que en otro puede que no esté permitido.

6.4.2. Competencia Judicial Internacional: especial referencia a España

En este contexto se plantean tres cuestiones esenciales[971], aplicables a las relaciones jurídicas internacionales:

- La competencia de un foro o jurisdicción internacional, para resolver la controversia.

- El problema del derecho aplicable (derecho aplicable por elección de partes o por designación de la norma de conflicto).

- El reconocimiento y ejecución de una sentencia, resuelta en jurisdicción extranjera.

Para el derecho es relevante definir cuando la relación jurídica fue consecuencia de una acción intencionada, fortuita o involuntaria, ya que trae consigo soluciones normativas diferenciadas.

[971] CALVO CARAVACA, A. L. y CARRASCOSA GONZÁLEZ, J.: *Derecho internacional privado*, Granada, 2013, pág. 95 y ss.

Entonces, si conectamos la circunstancia práctica de la acción, desempeñada por las partes y la necesidad de saber a qué Tribunal puede atribuirse el juzgamiento de un caso, vemos la importancia que tiene para la regulación de los derechos, fijar cuál o cuáles han sido los sitios de las actividades, que han dado lugar al conflicto, por la acción de las partes. A lo anterior hay que añadir, la presencia de un elemento extranjero, que hace importante adoptar una adecuada planificación de una estrategia global para resolver la situación de carácter internacional.

Contratar a través de internet provoca la transnacionalidad de los derechos[972], siendo esta su característica esencial, porque el traspaso permanente de fronteras implica el cruce de derechos de diferentes soberanías cuando aparece la controversia. Ante las situaciones planteadas, para encontrar una solución, nos fijaremos en nuestro ordenamiento jurídico. De esta forma, una primera consideración que hemos de tener presente es la adecuada planificación de la estrategia del asunto internacional que nos atañe.

Si se decide iniciar un proceso judicial se debe valorar muy detenidamente si hacerlo en España o en el extranjero. No obstante, puede ocurrir que la presencia de un elemento extranjero, en la situación jurídica ni siquiera aconseje resolver ésta desde la perspectiva del sistema de Derecho Internacional Privado, bastando hacerlo desde el ángulo del sistema interno.

Litigar en el extranjero puede tener como ventaja principal, en el caso de vencer en el juicio, la inmediatez en la ejecución de la sentencia en el país del domicilio o de la residencia habitual del demandado, frente a la relativa dificultad de tener que ejecutar una sentencia en el extranjero. El inconveniente principal que nos encontramos es que litigaremos ante un sistema judicial y jurídico extranjero, que, generalmente, es desconocido y, además, nos encontraríamos con una tendencia natural de los órganos judiciales a decantarse a favor de sus nacionales, frente a los extranjeros. Por otro lado, litigar en el Estado del foro, es decir, litigar en España, tiene las ventajas y los inconvenientes inversos a los de litigar en el extranjero. Por ello sería aconsejable, en la medida de lo posible, que el pleito sea iniciado en España ante los jueces españoles,

[972] MASON, S.: *Electronic signature in Law,* Cambridge, 2012, pág. 176 y ss.

aunque después resulte preciso tener que reconocer la sentencia vencedora en un Estado extranjero (factor que habría que valorar detenidamente; pues, puede resultar complicado o imposible reconocer la sentencia española en tal Estado).

En este planteamiento, debemos tener presente la posibilidad de ser el primero en presentar la demanda ante los órganos judiciales españoles, en lo que la doctrina ha venido a llamar la "carrera hacia el Tribunal", que da un avanzado paso en pro de vencer en el fondo; pues, obliga a la otra parte a seguir su estrategia procesal sin apenas otro arma disponible para contrarrestarla que la litispendencia. Aunque, también, cabe que se realice al contrario, creando el problema al residente español.

Un primer medio procesal de defensa es interponer, en la contestación a la demanda, la llamada excepción de incompetencia de jurisdicción que, no obstante, no siempre puede ser utilizada. En ocasiones, el órgano judicial extranjero, ante el que se presenta la demanda, controla de oficio su competencia judicial internacional en el asunto en cuestión, no siendo preciso que el demandante alegue su eventual incompetencia. Así, ocurre en los instrumentos supraestatales más relevantes en la materia, para evitar que un órgano judicial conozca bien de asuntos que son de la competencia exclusiva de otro órgano (Artículos 25 del Reglamento 44/2001 o 19 del Convenio de Bruselas de 1968), bien de casos en los que el demandado no ha comparecido tras notificársele la demanda, resultando que el órgano judicial ante el que se presentó la demanda no es competente, en virtud de ninguno de los foros consagrados en el instrumento internacional de que se trate (Artículos 26, 1 del Reglamento 44/2001 o 20,1 del Convenio de Bruselas de 1968).

Una especial importancia adquiere, en este punto, la sumisión, tanto expresa como tácita. Así, si se ha pactado la atribución de competencia judicial internacional a los órganos judiciales de un concreto Estado y una de las partes, en dicho pacto, presenta una demanda ante otro órgano judicial, el demandado puede alegar la competencia exclusiva de aquéllos y, en consecuencia, la incompetencia de éste (Artículos 22,1 del Reglamento 44/2001 o 17,1 del Convenio de Bruselas de 1968). Si el demandado compareciera, contestando la demanda, en cuanto al fondo, no alegando el pacto de sumisión, se estaría sometiendo tácitamente a dicho órgano judicial (Artículos 24 del Reglamento 44/2001 o 18 del Convenio de Bruselas de 1968), siendo frecuente en la

práctica que el demandante extranjero presente su demanda ante un órgano judicial que no es competente, pero que le resulta mucho más cercano o favorable para provocar en el demandado la sumisión tácita, que prevalece incluso sobre la expresa. Por ello, es necesario impugnar siempre la competencia judicial internacional, antes de contestar al fondo, de manera subsidiaria.

Posteriormente, hemos de pasar a determinar la competencia judicial. Debemos tener claro, que a través de la competencia judicial internacional, se determina solo el Estado cuyos órganos judiciales serán, en general, competentes para conocer de un asunto, siendo una cuestión distinta, y puramente interna, la de determinar la competencia territorial concreta de entre sus distintos órganos judiciales.

El legislador de cada Estado determina la competencia judicial internacional de sus Tribunales, mediante los llamados foros o criterios de competencia judicial internacional. A través de los mismos, se pone de relieve, la existencia de una cierta conexión del litigio con un Estado, que en España se regula en los Artículos 21 y 25 de la Ley Orgánica del Poder Judicial[973], que consagran nuestro sistema de competencia judicial internacional aplicable, en defecto de regulación supraestatal.

Con frecuencia, los legisladores estatales atribuyen a sus Tribunales un volumen excesivo o exorbitante de competencia judicial internacional, en cuyo caso, estaríamos ante los llamados foros exorbitantes, que no denotan una conexión suficiente del litigio con aquéllos. En el ámbito europeo existen mecanismos para luchar contra estos foros, a través de regulaciones contenidas en instrumentos internacionales (Artículo 3.2 del Reglamento 44/2001 o del Convenio de Bruselas de 1968), con el objetivo de que no resulten favorecidos, en la práctica, los litigantes de un Estado frente a los de otros.

Visto lo anterior, es necesario comprobar si es de aplicación al caso o no, algún instrumento internacional en el que España sea parte. Tratándose de competencia judicial internacional, conviene siempre comprobar si es de aplicación el Reglamento 44/2001, para lo cual se ha de verificar, en primer lugar, si el comercio electrónico y la firma electrónica son materias excluidas del ámbito material de aplicación por el

[973] Concretamente en artículo 22 LOPJ establece criterio de competencia el domicilio del demandado y, en cualquier otro caso, el lugar de celebración del contrato.

Artículo 1, que como sabemos no lo son; en segundo, hemos de verificar si el demandado está domiciliado o no o tienen algún vínculo con un Estado parte en el Reglamento 44/2001.

De darse los criterios de aplicabilidad del Reglamento 44/2001 la solución vendrá dada por el marco jurídico de este instrumento, sin que haya que recurrir al sistema autónomo español de competencia judicial internacional, que como hemos comentado, se encuentra regulado en los Artículos 21 y siguientes de la Ley Orgánica del Poder Judicial. Así, en la aplicación del mencionado Reglamento habrá de recurrir al sistema jerárquico de foros de competencia establecidos en los Artículos 22 y siguientes.

6.4.3. Forum non conveniens

Contratar a través de Internet provoca transnacionalidad de derechos[974]. Ante la posibilidad de que no resulte aplicable el planteamiento desarrollado en el apartado anterior, resulta necesario tener en cuenta, que el método clásico de determinación del órgano judicial competente y del ordenamiento aplicable al fondo de un supuesto de tráfico externo, que se asienta en las variables de la naturaleza del supuesto y de las circunstancias del caso concreto, continúa aferrándose a la utilización de criterios, mayoritariamente, rígidos, generales y, a menudo, territoriales que no permiten señalar, de un modo previsible y justo, la Ley aplicable o la jurisdicción competente en los supuestos litigiosos que surgen en Internet, que son casos de alcance planetario; esto es, conectados con infinidad de países[975].

Dicho esto, tenemos claro que cada Estado determina sus propias normas y procedimientos. Estas leyes se denominan *lex fori* o la ley del foro. De esta forma, el

[974] Asimismo, debemos tener en cuenta que se pueden plantear problemas cuando se quieren encajar criterios tradicionales de localización territorial para determinar la competencia judicial internacional o conexiones de corte territorial, para designar la ley aplicable a las relaciones privadas internacionales; habida cuenta que éstas relaciones ya no se generan en el marco de una sociedad industrial, sino en el marco de una sociedad digital. De esta forma, criterios como el domicilio del demandado, lugar de celebración del contrato o residencia habitual del prestador característico requieren de una reformulación (DIAGO DIAGO, Mª.P.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario LA LEY*, núm. 8432, 2014).

[975] CALVO CARAVACA, A. L. y J. CARRASCOSA GONZALEZ, J.: *Conflictos de Leyes y conflictos de jurisdicciones en internet*, Madrid, 2001, pág. 24 y ss.

sistema judicial de cada país debe determinar a fondo el procedimiento civil propio, cuándo y cómo se debe aceptar la competencia.

Por lo general, un Tribunal estatal solamente puede adquirir jurisdicción sobre personas físicas o personas jurídicas, que se encuentren físicamente dentro de su territorio, por lo que éste no tiene jurisdicción sobre personas que no se encuentren físicamente presentes dentro de su propio territorio geográfico.

No obstante, en el caso *International Shoe v. Washington*[976], el Tribunal Supremo de los Estados Unidos amplió la red de la jurisdicción para incluir a personas físicamente ausentes de un territorio estatal, siempre y cuando éstas tengan ciertos contactos mínimos con el Estado; es decir, contactos por medio de los cuales el demandado comete actos, que directamente impactan sobre dicho Estado y sus residentes.

Dichos contactos tienen que ser lo suficientemente sustanciales para que un Tribunal pueda compeler la presencia del demandado y adquirir jurisdicción sobre su persona, sin ofender las nociones sustanciales de trato justo y justicia sustancial. El Tribunal, también, aclaró que la relación que existe entre un demandado y el foro, tiene que ser de tal naturaleza, que fuese razonable requerir a dicho demandado a que se defienda en ese foro.

Ante esta situación se torna forzosa que los Tribunales tengan que acudir a la naturaleza y cantidad de los contactos con el foro. Sin embargo, la existencia o inexistencia de contactos mínimos de un demandado, no residente, con determinado foro, no goza de certeza jurídica alguna, ya que estas determinaciones se hacen basándose en los hechos específicos de cada caso.

De esta forma, el problema surge en el momento en que se procede a la elección del foro para conocer de una acción. Así, cuando ante un Tribunal se presenta una controversia con elementos de extranjería, se debe examinar si se tiene jurisdicción y competencia, tanto sobre la materia, como sobre las personas.

[976] ESTADOS UNIDOS: Caso International Shoe v. Washington, 326 U.S. 310 (1945).

En los países con tradición de *common law* este dilema se ha atendido, adoptando los llamados *long arm statutes*[977], o estatutos que permiten extender la jurisdicción personal sobre quienes hacen gestiones de negocios desde otro Estado. Esto no constituirá la determinación de jurisdicción y competencia. Se entra a considerar si el foro local es el más adecuado o conveniente para atender la controversia, aunque tenga jurisdicción y sea competente. Esto, con el propósito de evitar que un Tribunal tenga que atender controversias, con las cuales tiene poca relación o interés. Los criterios, para esta determinación, los provee la doctrina de *forum non conveniens*[978].

Si el Tribunal determina que no es el foro más apropiado, desestimará la demanda, para que sea presentada ante el Tribunal más adecuado o paralizará los procedimientos, hasta que la controversia sea resuelta en el otro Tribunal. Para determinar si, al declarar como lugar la moción de *forum non conveniens*, procede la desestimación o la paralización de los procedimientos, se debe aplicar la normativa estatutaria y jurisprudencial de la jurisdicción donde se presentó la petición.

En Inglaterra, Australia y Canadá los Tribunales paralizan los procedimientos, como norma general, hasta que se demuestre que los Tribunales del foro alternativo entendieron sobre el asunto controvertido. Una vez demostrado, dictarán la desestimación. Por el contrario, en Estados Unidos, una vez se declara que da lugar a la moción de *forum non conveniens*, en la mayoría de los casos, se desestimaran la demanda a favor del foro alternativo[979].

Cuando el Tribunal determine quién tiene jurisdicción y quién debe ejercerla, será necesario, también, caracterizar o calificar el caso y decidir cuál es la Ley aplicable,

[977] Long arm statutes: es una disposición legal que permite al Estado ejercer su jurisdicción sobre un acusado fuera de su estado, siempre y cuando el posible demandado tiene suficientes contactos mínimos con el Estado del foro. Competencia general significa que el poder de un tribunal para escuchar y tomar una decisión en una situación dada. Hay diferentes categorías de jurisdicción en jurisdicción; rem, en personam o jurisdicción personal, competencia en la materia, la jurisdicción original y jurisdicción independiente son los que más se debaten. Un ejemplo podemos encontrarlo en el Washington Long-Arm Statute (Wash. Rev. Code § 4.28.185).
Disponible en: http://definitions.uslegal.com/l/long-arm-statute/ (última visita: 3/102014).
Diponible en: http://www.lrcvaw.org/laws/walongarm.pdf (última visita: 27/5/2014).

[978] PUERTO RICO: Sentencia la Corte Suprema de Puerto Rico de 6 de octubre de 2009 (Caso nº: CC-2005-553).

[979] DAVIES, M.: "Time to Change the Federal Forum Non Conveniens Analysis", *LexisNexis Review*, 2002, núm.309, pág.77.

según las normas de Derecho Internacional Privado local. Calificar o caracterizar, en el contexto del Derecho Internacional Privado, es introducir los hechos en un concepto jurídico; es decir, determinar conforme a qué tipo de normas se va a resolver el caso[980].

Esta doctrina conocida como *forum non conveniens* es una doctrina propia del sistema del *common law*, que permite a un Tribunal declinar el ejercer su función jurisdiccional si un foro alternativo sería sustancialmente más conveniente o apropiado.

Esta doctrina tuvo su origen en Escocia, con el fin de poder contrarrestar el indebido gravamen que surgía por el embargo y desposesión de bienes extranjeros, con el objeto de forzar a los extranjeros a comparecer antes los Tribunales escoceses[981]. Para desestimar las causas, además, de que el foro fuera poco práctico, se requería que hubiese otro Tribunal de jurisdicción competente, en donde los casos pudieran ser ventilados de manera más adecuada a los intereses de todas las partes y de los fines de la justicia. En este sentido, cobra especial relevancia el primer reconocimiento con fuerza de autoridad de la Sentencia del Tribunal Supremo de Estados Unidos sobre la doctrina que se dio, concretamente, en el caso *Gulf Oil Corp. v. Gilbert*[982].

En este caso, el alto Tribunal de Estados Unidos adoptó unos criterios a fin de poder aplicar la doctrina *forum non conveniens*, si bien comentó que había que tener un especial cuidado; pues, hay que limitar la desestimación a casos inusuales, en los cuales un demandante realmente no busca justicia, sino que acosa u hostiga al demandado. Así, antes de considerar la procedencia de una solicitud de esta naturaleza, los Tribunales deben establecer su jurisdicción y competencia, para luego determinar que existe al menos otro foro con jurisdicción sobre los demandados. Por consiguiente, es un requisito de umbral, asegurar que hay un foro alternativo disponible.

Asimismo, estableció ciertos factores privados y públicos, que se deben sopesar al considerar en una petición de esta naturaleza. Entre los privados incluyó el lugar donde residen los testigos y la disponibilidad de recursos para obligarlos a comparecer a juicio,

[980] RIGAUX, F.: *Derecho Internacional Privado: Parte General*, Madrid, 1985, págs. 94 y ss.
[981] FEDELSTEIN DE CARDENAS, S. L.; SCOTI, L. B.: "Asunción de los medios electrónicos en la Ley panameña sobre litigios internacionales", en *Contratación electrónica internacional: una mirada desde el derecho internacional privado* (Dir. Fedelstein de Cárdenas), Buenos aires, 2008, pág. 307 y ss.
[982] ESTADOS UNIDOS: Caso Gulf Oil Corp. v. Gilbert - 330 U.S. 501 (1947).

el acceso a las fuentes de prueba, la posibilidad de realizar una inspección ocular, si ésta resulta necesaria y la posibilidad de poder ejecutar la sentencia. Entre los públicos están el interés del Estado y de la comunidad en que las controversias locales se decidan en su territorio, las dificultades administrativas, que surgen por la congestión de casos, y el problema que implica aplicar leyes extranjeras. Por último, debe respetarse la decisión del demandante, de seleccionar un determinado foro en la ponderación de intereses a favor de otro Tribunal.

Con posterioridad en el caso *Pipper Aircraft Co. v. Reyno*[983], adoptó un criterio contrario al establecido anteriormente, al considerar que para determinar la conveniencia del traslado a un Tribunal fuera de la jurisdicción estadounidense, se debe dar poco peso a la posibilidad de que el demandante quede afectado de manera desfavorable por razón del derecho aplicable en el foro alternativo; pues, la presunción a favor de la elección del foro, que el demandante solicita, es un riesgo razonable que debe asumir en la elección del foro, que, además, resulta conveniente. Así, el Tribunal Supremo de Estados Unidos resolvió que la decisión de declarar, si da lugar a denegar o no, una moción de *forum non conveniens*, quedará a la discreción del Tribunal y solamente puede revocarse cuando hay un claro abuso de esa discreción.

En los foros romanistas, esta doctrina del *forum non conveniens* no es siendo aceptada; pues, tiende a determinarse que si los tribunales tienen jurisdicción para entender sobre el asunto controvertido, éste no puede negarse a resolver la causa, salvo que se trate de una situación de litispendencia.

Así lo regula el Reglamento 44/2001, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[984], que sustituye al el Convenio de Bruselas de 1968[985], que en su Artículo 27 (Artículo 21

[983] ESTADOS UNIDOS: Caso Piper Aircraft Co. v Reyno - 454 EE.UU 235 (1981).
[984] Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/l33054_es.htm (última visita: 27/5/2014).
[985] Sigue siendo aplicable a los territorios de los Estados miembros que entran dentro de su ámbito de aplicación territorial y que están excluidos del presente reglamento con arreglo al artículo 299 del Tratado constitutivo de la Comunidad Europea (ahora artículo 355 del Tratado de Funcionamiento de la Unión Europea). El reglamento también enumera una serie de convenios, tratados y acuerdos celebrados entre los Estados miembros a los que sustituye. En el momento de la entrada en vigor del presente reglamento, la competencia judicial entre Dinamarca y los otros Estados miembros sigue estando regulada por el Convenio de Bruselas de 1968. Esta excepción para Dinamarca se basa en el protocolo n° 5 sobre la

del Convenio de Bruselas) establece que: "cuando se formularen demandas con el mismo objeto y la misma causa entre las mismas partes ante Tribunales de Estados contratantes distintos, el Tribunal ante el que se formulare la segunda demanda suspenderá de oficio el procedimiento en tanto no se declarare competente el Tribunal ante el que se interpuso la primera. Cuando el Tribunal ante el que se interpuso la primera demanda se declarare competente, el Tribunal ante el que se interpuso la segunda se inhibirá a favor de aquél". De esta forma, la admisión de la litispendencia evita la coexistencia de dos decisiones sobre la misma causa incompatibles entre sí, por tanto, para la libre circulación de decisiones.

Para su aplicación es necesario que las demandas se hayan presentado ante tribunales de Estados contratantes distintos. La solución consiste en optar por el Tribunal ante el que se ha iniciado con anterioridad el procedimiento, entendiendo por aquél la jurisdicción, ante la cual se cumplimentaron, en primer lugar, las condiciones, que permitieron concluir en una litispendencia definitiva, debiendo ser apreciadas dichas condiciones, según la Ley nacional de cada una de las jurisdicciones implicadas.

Así, a efectos de la aplicación del *forum non conveniens* el Artículo 2 del Reglamento 44/2001[986] (así como el Convenio de Bruselas), determina que el carácter internacional de la relación jurídica de que se trate, no tiene que derivar necesariamente en la implicación de varios Estados contratantes, debido al fondo del litigio o al domicilio respectivo de las partes del litigio. El hecho de que estén implicados un Estado contratante y un tercer Estado, debido a que el demandante y uno de los demandados están domiciliados en el primer Estado y a que los hechos controvertidos

posición de Dinamarca de 1997, anexo a los Tratados (ahora Protocolo nº 22). El 19 de octubre de 2005, la UE firmó un acuerdo con Dinamarca extendiendo las disposiciones del presente reglamento en materia civil y mercantil a este país. El 27 de abril de 2006, el acuerdo fue aprobado en nombre de la UE mediante la Decisión del Consejo 2006/325/CE que entró en vigor el 1 de julio de 2007. Tal como se prevé en el Protocolo sobre la posición del Reino Unido y la República de Irlanda anexo a los Tratados, ambos países notificaron su deseo de participar en la adopción y aplicación del presente Reglamento. Disponible en:
http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/l33054_es.htm (última visita: 27/5/2014).

[986] Artículo 2 del Reglamento 44/2001: "1) Salvo lo dispuesto en el presente Reglamento, las personas domiciliadas en un Estado miembro estarán sometidas, sea cual fuere su nacionalidad, a los órganos jurisdiccionales de dicho Estado; 2) A las personas que no tuvieren la nacionalidad del Estado miembro en que estén domiciliadas les serán de aplicación las reglas de competencia judicial que se aplicaren a los nacionales".

se han producido en el segundo Estado, también puede conferir carácter internacional a la relación jurídica de que se trate.

Una situación de este tipo puede plantear en el Estado contratante, como sucede en el procedimiento principal, cuestiones relativas a la determinación de la competencia de los órganos jurisdiccionales en el orden internacional, lo que constituye precisamente uno de los objetivos del Convenio de Bruselas, como se desprende del tercer Considerando de su preámbulo. No obstante, las reglas uniformes de competencia contenidas en el Convenio de Bruselas no se aplican únicamente a las situaciones que tienen un vínculo efectivo y suficiente con el funcionamiento del mercado interior, el cual, implica, por definición, a varios Estados miembros[987].

De esta manera, el Tribunal de Justicia de la Unión Europea no admite matices a la inclusión de esta excepción. Así, en Sentencia de 1 de marzo de 2005[988], señala que el Artículo 2 tiene carácter imperativo y, como se desprende de su tenor, las únicas excepciones a la regla de principio que contiene, son las que están expresamente contenidas en dicho Convenio[989]. Pues bien, consta que el Convenio no prevé una excepción basada en la teoría del *forum non conveniens*, a pesar de que la cuestión fue debatida al elaborarse el Convenio de 9 de octubre de 1978 relativo a la adhesión de Dinamarca, Irlanda y Reino Unido, como se desprende del informe sobre dicho Convenio[990].

El respeto del principio de seguridad jurídica, que constituye uno de los objetivos del Convenio de Bruselas[991], no quedaría plenamente garantizado si hubiera que permitir que un órgano jurisdiccional competente, con arreglo al mencionado Convenio, aplicara la excepción de *forum non conveniens*.

---

[987] OTERO GARCÍA-CASTRILLÓN, C.: "COMPETENCIA JUDICIAL: Convenio de Bruselas. Ámbito de aplicación territorial. Normas nacionales de aplicación. Forum non conveniens", en "Jurisprudencia española y comunitaria de derecho internacional privado" (Coord. y Selección ÁLVAREZ GONZÁLEZ, S.), *Revista de Derecho Internacional Española*, 2005, vol. LVII, 2, págs. 925 – 986.

[988] UNIÓN EUROPEA: Sentencia del Tribunal de Justicia de la Unión Europea 1 de marzo de 2005 (as. C-281/02, caso Andrew Owusu c. N. B. Jackson).

[989] Sentencia del Tribunal de Justicia de la Unión Europea de 9 de diciembre de 2003 (Gasser, C116/02).

[990] Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61999CO0518:ES:HTML
(última visita: 27/5/2014).

[991] UNIÓN EUROPEA: Sentencia del Tribunal de Justicia de la Unión Europea de 28 de septiembre de 1999 (GIE Groupe Concorde y otros, C440/97).

Como comenta el TJUE, en la citada Sentencia, el Convenio de Bruselas tiene como objetivo fortalecer, en la Comunidad, la protección jurídica de las personas establecidas en la misma, previendo reglas comunes de competencia que proporcionen certeza, por lo que se refiere a la distribución de competencias entre los diferentes Tribunales nacionales, que pueden conocer de un determinado litigio. Así, el principio de seguridad jurídica exige, en particular, que las reglas de competencia que establecen excepciones al principio general enunciado en el Artículo 2 del Convenio de Bruselas se interpreten de modo que permitan al demandado, normalmente informado, prever razonablemente, cuál es el órgano jurisdiccional distinto al del Estado de su domicilio, ante el que pudiera ser demandado.

Además, la aplicación de la teoría del *forum non conveniens*, deja un amplio margen de apreciación al juez, que conoce del asunto, para decidir si un foro extranjero es más adecuado para resolver el fondo del litigio, puede afectar a la previsibilidad de las reglas de competencia establecidas en el Convenio de Bruselas, en particular, la de su Artículo 2, y, por consiguiente, de nuevo, al principio de seguridad jurídica como fundamento de dicho Convenio.

Si se aceptara la excepción de *forum non conveniens*, en el marco del Convenio de Bruselas, pondría en peligro la aplicación uniforme de las reglas de competencia que éste contiene, en la medida en que solamente un número limitado de Estados contratantes reconoce dicha excepción, siendo, así, que el objetivo del Convenio es precisamente establecer reglas comunes y excluir las reglas nacionales exorbitantes.

Ante esta situación, es obligatorio preguntarse si sería conveniente o no aceptar la teoría del *forum non conveniens*, en los asuntos referentes al comercio electrónico y a la firma electrónica, teniendo en cuenta la necesidad de reconocimiento jurídico internacional, para evitar los obstáculos que impiden su desarrollo.

En los países con tradición de *common law* se ha producido la extensión de esta doctrina. Un ejemplo, lo encontramos en Estados Unidos, aunque las controversias aún no han llegado al Tribunal Supremo y, por tanto, aún no se ha establecido precedente normativo alguno, si hay casos resueltos en los diferentes Estados de la Unión.

La mayoría han seguido la decisión adoptada por el Tribunal del Distrito Federal para el Distrito Oeste de Pensilvania en el caso *Zippo Manufacturing Co. v. Zippo Dot Com*[992], donde el Tribunal estableció las bases conceptuales de la doctrina, cuando una entidad intencionalmente, a través de Internet, llega a alcanzar un foro que se encuentra fuera de los límites geográficos de su Estado de residencia, para realizar negocios con los residentes de ese otro Estado, es apropiado ejercer la jurisdicción personal de esta persona, en el foro que le es físicamente ajeno. De esta forma, matiza que el Tribunal Supremo de los Estados Unidos decretó, en el *caso McGee v. International Life Insurance Co*[993], que un sólo contacto, que sea sustancial, puede ser suficiente para ejercer la jurisdicción *in personam* sobre un demandado. Así, nos dice que esta doctrina siempre se ha enfocado en la naturaleza y calidad de los contactos con el foro y no en la cantidad de esos contactos.

Otro ejemplo, lo encontramos en el caso *Dow Jones v. Gutnick*[994], en el que, por primera, vez se pronunció el Tribunal Superior de Australia acerca de la cuestión de la jurisdicción sobre las actividades de Internet. El resultado de los hechos del caso fue que un residente del Estado de Victoria (Australia) tiene derecho a demandar en este Estado, respecto de los daños que ha sufrido por la publicación de un artículo en Internet en Nueva Jersey (Estados Unidos). El enfoque, basado en si el editor acusado trató de perjudicar a la demandante en el foro, establece un equilibrio más en los casos de difamación de Internet, entre los derechos de los demandantes y demandados. De esta forma, tratan de asegurar que los Tribunales australianos tengan competencia sobre cualquier tipo de actividad, que pueda llevarse a cabo vía Internet, partiendo de una base amplia, fijando como criterio el mencionado contacto mínimo; pues, de lo contrario, el resultado sería perjudicial para la cortesía entre los Estados y también, posiblemente, llevar Australia a convertirse en un imán para los litigios por difamación o cualquier otra materia relacionada, con la transferencia de datos a nivel internacional.

En los foros romanistas, sin embargo, parece poco probable que se adopte esta doctrina, que permitiría, en algunos casos, resolver el problema que venimos

[992] ESTADOS UNIDOS: Caso Zippo Fabr. Co. v Zippo Dot Com, Inc., 952 F. Supp. 1119 (1997).
[993] ESTADOS UNIDOS: McGee v. International Life Insurance Co., 355 U.S. 220 (1957).
[994] AUSTRALIA: Caso Gutnick v Dow Jones & Co Inc [2002] HCA 56; (2002).

planteando. Esto es así, porque, como hemos dicho anteriormente, las reglas en vigor en la Unión Europea, en particular, el Reglamento 44/2001, en su Artículo 23, no ofrece una cobertura efectiva a la autonomía de las partes en materia de elección del foro[995].

Con la obligación del juez designado por las partes de suspender el procedimiento con carácter previo, sí se ha presentado la demanda ante otro juez, permite que las partes que actúen de mala fe, puedan retrasar la resolución del litigio ante el juez elegido, acudiendo previamente a un juez incompetente, generando costes y retrasos adicionales, además de socavar la seguridad jurídica y la previsibilidad en la resolución de tales controversias[996].

Ante esto, surge la necesidad de que se admita la flexibilidad de conexiones de competencia; por ello, en nuestra opinión, surge la necesidad de fijar la atribución de jurisdicción, cuando el demandado no es residente en el lugar del foro[997]; es decir,

[995] BEAUMONT, P.; YÜRSEL, B.: "La reforma del Reglamento de Bruselas I sobre acuerdos de sumisión y la preparación para la ratificación por la UE del Convenio de la Haya sobre acuerdos de elección de foro", en *Anuario español de derecho internacional privado*, tomo IX, 2009, págs. 129 – 159.

[996] SALVATORI, M.: "El Convenio sobre Acuerdos de Elección del Foro y el Reglamento Bruselas I: autonomía de la voluntad y procedimientos paralelos", en *Anuario español de derecho internacional privado*, tomo X, 2010, págs. 829 – 844.

[997] Resulta interesante destacar la STJUE de 25 de octubre de 2011 asuntos acumulados C-509/09 y C-161/10, eDate Advertising GmbH vs Olivier Martinez, Robert Martinez y MGN Limited, que en lo que se refiere hace una interpretación amplia del Artículo. 5,3 del Reglamento 44/2001 (Artículo 7,2 del nuevo Reglamento 1215/2012), al realizar las siguientes consideraciones: "Las dificultades de la aplicación, en el contexto de Internet, del citado criterio del lugar donde se ha producido el daño. Por lo tanto, procede adaptar los criterios de conexión recordados en el sentido de que la víctima de una lesión de un derecho de la personalidad a través de Internet puede acudir, en función del lugar en el que haya producido el daño causado en la Unión Europea por dicha lesión, a un fuero por la totalidad de ese daño. Habida cuenta de que la repercusión de un contenido publicado en Internet sobre los derechos de la personalidad de una persona puede ser apreciada mejor por el órgano jurisdiccional del lugar en el que la supuesta víctima tiene su centro de intereses, la atribución de competencia a dicha órgano jurisdiccional corresponde al objetivo de una buena administración de la justicia. Por lo general, el lugar en el que una persona tiene su centro de intereses corresponde a su residencia habitual. Sin embargo, una persona puede tener su centro de intereses también en un Estado miembro en el que no resida habitualmente, en la medida en que otros indicios, como el ejercicio de una actividad profesional, permitan establecer la existencia de un vínculo particularmente estrecho con ese Estado miembro. La competencia del órgano jurisdiccional del lugar en el que la presunta víctima tiene su centro de intereses es conforme con el objetivo de la previsibilidad de las normas de competencia (véase la sentencia de 12 de mayo de 2011, BVG, C-144/10, Rec. p. I-0000, apartado 33) también con respecto al demandado, dado que el emisor de un contenido lesivo puede, en el momento de la publicación en Internet de ese contenido, conocer los centros de intereses de las personas que son objeto de éste. Por lo tanto, procede considerar que el criterio del centro de intereses permite, al mismo tiempo, al demandante determinar fácilmente el órgano jurisdiccional ante el cual puede ejercitar una acción y al demandado prever razonablemente ante qué órgano jurisdiccional puede ser demandado (véase la sentencia de 23 de abril de 2009, Falco Privatstiftung y Rabitsch, C-533/07, Rec. p. I-3327, apartado 22 y jurisprudencia citada). Por otra parte, en vez de una acción basada en la responsabilidad por la totalidad del daño, el criterio del lugar donde se ha producido éste, consagrado en la sentencia Shevill y otros, antes citada, otorga competencia a los órganos jurisdiccionales de cada Estado miembro en cuyo territorio un contenido publicado en Internet

cuando se determina la competencia en base a criterios especiales o bajo la óptica de la teoría de los contactos mínimos y razonables (*forum non conveniens*).

Esta parece ser la postura adoptada tras la firma del Convenio de La Haya sobre Acuerdos de Elección del Foro[998], de 2005, por la Unión Europea. Este Convenio supone un efecto positivo que se manifiesta con la propuesta de modificación del Reglamento 44/2001[999], y la posterior aprobación del Reglamento 1215/2012[1000], de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, elaborada por la Comisión europea, en el que: por un lado, se supera la remisión a las normas estatales de competencia, cuando el demandado esté domiciliado en un tercer Estado; y por otro, se atribuye una mayor eficacia a los acuerdos atribuidos de competencia[1001].

Con este Reglamento 1215/2012[1002] se dispone que el juez designado sea el que se pronuncie, prioritariamente, sobre su propia competencia, incluso si entra a conocer en segundo lugar y que la validez del acuerdo se determine de conformidad con la Ley designada por una norma de conflicto uniforme, en lugar de aplicar las normas del foro.

Con ello, se pretende evitar que la remisión a las normas estatales de competencia, en lo que respecta a las demandas presentadas frente a domiciliados en terceros Estados, sin que comporte un obstáculo al buen funcionamiento del mercado, favoreciendo el *forum shopping*, basado en la disparidad de las legislaciones nacionales y susceptible de tener repercusiones, no sólo en las relaciones entre personas domiciliadas y no

---

sea, o haya sido, accesible. Dichos órganos son competentes para conocer únicamente del daño causado en el territorio del Estado miembro de la jurisdicción a la que se haya acudido."
Disponible en: http://curia.europa.eu/juris/liste.jsf?language=es&num=C-509/09 (última visita: 11/12/2014).

998 Disponible en: http://www.hcch.net/index_es.php?act=conventions.text&cid=98#_ftn1 (última visita: 27/5/2014).

999 Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001R0044:20090408:ES:PDF (última visita: 27/5/2014).

1000 Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:ES:PDF (última visita: 27/5/2014).

1001 BORRÁS, A..: "La aplicación del Reglamento Bruselas I a domiciliados en terceros estados: los trabajos del grupo europeo de derecho internacional privado", en *Anuario español de derecho internacional privado*, Tomo X, 2010, págs. 829 – 844.

1002 Artículo 81 del Reglamento 1215/2012: "Será aplicable a partir del 10 de enero de 2015, con excepción de los artículos 75 y 76, que serán aplicables a partir del 10 de enero de 2014".

domiciliadas en la Unión Europea, sino también entre personas domiciliadas en la propia Unión Europea.

De esta forma, se ha previsto un mecanismo claro y eficaz que permite resolver los casos de litispendencia y conexidad y de obviar los problemas derivados de las divergencias nacionales, por lo que respecta a la determinación de la fecha en la que un asunto se considera pendiente. A efectos del presente Reglamento es oportuno definir esa fecha de manera autónoma.

Sin embargo, a fin de mejorar la eficacia de los acuerdos exclusivos de elección de foro y de evitar las prácticas litigiosas abusivas es necesario prever una excepción a la norma general de litispendencia, para resolver satisfactoriamente una situación particular en la que se desarrollen procedimientos paralelos. Esta situación se produce cuando conoce del asunto, en primer lugar, un órgano jurisdiccional no designado en un acuerdo exclusivo de elección de foro y, a continuación, se somete ante el órgano jurisdiccional designado, una acción entre las mismas partes, con el mismo objeto y la misma causa. En tal caso, debe exigirse que el órgano jurisdiccional, que conoció del asunto, en primer lugar, suspenda el procedimiento tan pronto como la demanda se presente ante el órgano jurisdiccional designado y hasta que éste último se declare incompetente conforme al acuerdo exclusivo de elección de foro.

Se garantiza, así, que, en tal situación, el órgano jurisdiccional designado tenga prioridad para decidir sobre la validez del acuerdo y sobre el alcance de su aplicabilidad al litigio de que conoce. El órgano jurisdiccional designado debe poder actuar con independencia de que el órgano jurisdiccional no designado, ya se haya pronunciado sobre la suspensión del procedimiento.

El Reglamento 1215/2012 establece un mecanismo flexible que permite a los órganos jurisdiccionales, de los Estados miembros, tener en cuenta los procedimientos pendientes ante los órganos jurisdiccionales de terceros Estados, tomando especialmente en consideración, si las resoluciones de un tercer Estado podrán ser reconocidas y ejecutadas en el Estado miembro de que se trate, con arreglo a su legislación nacional y a la buena administración de justicia.

Por un lado, cuando entre en vigor el Convenio de La Haya sobre Acuerdos de Elección del Foro[1003], de 2005, permitirá a las partes en operaciones comerciales de todo el mundo elegir el juez al que someter, de forma exclusiva, los litigios que puedan surgir entre ellas. Este Convenio[1004] se lleva a cabo ante el deseo de promover el comercio y las inversiones internacionales, mediante el fortalecimiento de la cooperación judicial. La preocupación ya se advirtió en l997 cuando se convocó una Comisión Especial para estudiar los efectos de las decisiones de Tribunales extranjeros sobre cuestiones civiles y comerciales.

Así, surgió el Anteproyecto de Convenio sobre Competencia y Resoluciones Judiciales Extranjeras en Materia Civil y Comercial[1005], adoptada por la Comisión Especial, el 30 de Octubre de 1999, que tenía como objetivos, tanto la armonización de normas jurídicas sobre el reconocimiento y cumplimiento de decisiones judiciales, como fijar las bases donde pueden entablarse las acciones judiciales.

El Anteproyecto, en previsión del objetivo amplio de su enfoque y de las barreras territoriales, que, eventualmente, surgirán al regular la materia jurisdiccional, contemplaba dos normas esenciales, a los fines de la armonización de sistemas jurídicos, recepta la doctrina del *forum non convieniens* y establece cláusulas de compatibilidad de los derechos nacionales involucrados.

Este proyecto de Convenio, constituyó un ambicioso proyecto que buscaba asegurar dos de los problemas más complicados para otorgar eficacia a los derechos de las partes y que son parte del contenido del Derecho Internacional Privado: la eficacia de las sentencias en un Estado extranjero y las reglas de jurisdicción para litigios transnacionales.

[1003] De conformidad con el artículo 31 de la Convención es necesaria una segunda ratificación para que entre en vigor.
Situación actual del Convenio: http://www.hcch.net/index_es.php?act=conventions.status&cid=98 (última vista: 27/5/2014).

[1004] Disponible en: http://www.hcch.net/index_es.php?act=conventions.text&cid=98#_ftn1 (última visita: 27/5/2014).

[1005] ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL: *Información sobre el borrador preliminar del Competencia y Resoluciones Judiciales Extranjeras en Materia Civil y Comercial*, Ginebra, 28 de septiembre de 1999.

El resultado final del Convenio fue el refuerzo de la cooperación judicial, a través de reglas uniformes sobre competencia, reconocimiento y ejecución de resoluciones judiciales extranjeras en materia civil o comercial. Este fortalecimiento de la cooperación requiere, en particular, de un régimen jurídico internacional, que proporcione seguridad y asegure la eficacia de los acuerdos exclusivos de elección de foro entre las partes en operaciones comerciales y que regule el reconocimiento y la ejecución de resoluciones dictadas en los procedimientos basados en dichos acuerdos**.**

El Convenio se limita a acuerdos exclusivos de elección de foro en casos internacionales entre profesionales en asuntos civiles o comerciales (Artículo 1), con una extensión opcional del capítulo sobre el reconocimiento y la ejecución a las resoluciones dictadas por un Tribunal designado en un acuerdo no exclusivo de elección de foro (Artículo 22). Por ello, el Artículo 1 del Convenio en su párrafo primero establece tres condiciones para su aplicación: la internacionalidad de la situación, el carácter civil o comercial de la controversia y la existencia de un acuerdo exclusivo de elección del foro (en atención de lo previsto en el Artículo 22).

Por otro lado, el párrafo segundo establece que una situación no es internacional si las partes residen en el mismo Estado contratante y la relación entre éstas y, todos los demás elementos relevantes del litigio, cualquiera que sea el lugar del Tribunal elegido, están conectados únicamente con ese Estado. De esta forma, todos los casos, que presentan elementos de vinculación con diversos ordenamientos estatales, se consideran internacionales y entran en el ámbito de aplicación de la Convención. De lo contrario, estarán regulados por las normas del ordenamiento estatal, con el que se encuentran conectados[1006].

El Convenio contiene tres reglas principales referidas a diferentes Tribunales[1007]:

[1006] SALVATORI, M.: "El Convenio sobre Acuerdos de Elección del Foro y el Reglamento Bruselas I: autonomía de la voluntad y procedimientos paralelos", en *Anuario español de derecho internacional privado*, Tomo X, 2010, págs. 829 – 844.

[1007] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Reseña sobre el Convenio de la Haya sobre Acuerdos de Elección de Foro*, La Haya, 2009.
Disponible en: http://www.hcch.net/upload/outline37s.pdf (última visita: 27/5/2014).

a) El Tribunal elegido debe conocer del caso si el acuerdo de elección de foro es válido según las pautas establecidas por el Convenio (en particular no hay discreción/*forum non conveniens* a favor de los Tribunales de otro Estado) (Artículo 5).

b) Todo Tribunal, que conozca del asunto sin ser elegido, debe rechazar la demanda, salvo que resulta aplicable una de las excepciones establecidas por el Convenio (Artículo 6).

c) Cualquier resolución dictada por el Tribunal de un Estado contratante, que haya sido designado en un acuerdo exclusivo de elección de foro que sea válido según las pautas establecidas por el Convenio, debe ser reconocida y ejecutada en los demás Estados contratantes (Artículo 8), salvo si fuese aplicable una de las excepciones establecidas en el Convenio (Artículo 9).

En la actualidad[1008], el Convenio ha sido ratificado únicamente por México, el 26 de noviembre de 2007, y firmado por Estados Unidos, el 19 de junio de 2009 y por la Unión Europea[1009], en nombre de todos los Estados miembros, a través de la Decisión del Consejo de 29 de febrero de 2009[1010].

[1008] Disponible en: http://www.hcch.net/index_es.php?act=conventions.status&cid=98 (última visita: 27/5/2014).

[1009] La Unión Europea declara que, de conformidad con el artículo 30 del Convenio, que ejerce competencia para todas las materias regidas por esta Convención. Sus Estados miembros no pueden firmar, ratificar, aceptar o aprobar la Convención, pero estarán obligados por el Convenio. A los efectos de esta declaración, el término Unión Europea no incluye a Dinamarca por virtud de los artículos 1 y 2 del Protocolo sobre la posición de Dinamarca anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea.
Disponible en:http://www.hcch.net/index_es.php?act=status.comment&csid=1044&disp=resdn (última visita: 27/5/2014).

[1010] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:133:0001:0013:ES:PDF(última visita: 27/5/2014).

6.4.4. Los mecanismos extrajudiciales de solución de controversias

El comercio electrónico va unido a la expansión de conflictos de alcance transfronterizo, implicando transacciones de escaso valor, bienes específicos de Internet y condicionadas por la configuración de la red. Las peculiares características de los conflictos surgidos en el ámbito del comercio electrónico, unido al potencial de las vías electrónicas para la rápida y eficaz resolución de controversias, contribuyen a la importancia atribuida al empleo de mecanismos extrajudiciales en un entorno electrónico. La creación de estos mecanismo de solución de controversias, desarrollados en línea y configurados como una alternativa voluntaria y no excluyente del ejercicio de acciones ante tribunales estatales, reviste especial importancia en relación con las transacciones típicas de comercio electrónico, en particular, en situaciones transfronterizas donde no existen mecanismos de arbitraje, en sentido propio, disponibles, al menos, en sistemas tan restrictivos como el español[1011].

Reconociendo el valor del arbitraje, como medio para solucionar controversias, nacidas de las relaciones comerciales internacionales y el desarrollo de las tecnologías de la comunicación, resulta fundamental, para que los consumidores y las empresas dispongan de instrumentos para resolver los litigios, sobre todo, si las partes se encuentran en jurisdicciones diferentes. La experiencia acumulada, con los métodos tradicionales de solución de litigios, es esencial para el desarrollo de procedimientos en un entorno electrónico.

Se están elaborando numerosos mecanismos en los que se combinan los métodos tradicionales con las ventajas de las nuevas tecnologías. Entre otras cosas, porque esto mejora el acceso a esos mecanismos, agiliza el proceso y ofrece a las partes un mayor control del procedimiento de resolución. Las tecnologías tendrán una función cada vez más central en la resolución de litigios y podrían contribuir a ofrecer una alternativa verosímil al procedimiento judicial. Será un importante factor para consolidar la confianza de los consumidores y las empresas en el mercado interior[1012].

[1011] DE MIGUEL ASENSIO, P.A.: *Derecho Privado de Internet*, Madrid, 2011, págs. 971 y ss.
[1012] COMISIÓN EUROPEA: *Comunicación relativa a la mejora del acceso de los consumidores a mecanismos alternativos de solución de litigios (COM/2001/0161 final)*, Bruselas, 4 de abril de 2001.

En esta situación, la aplicación de las nuevas tecnologías y herramientas de la comunicación a las fases de los procedimientos de ADR (Alternative Dispute Resolution) tradicionales, surgen las ODR (Online Dispute Resolution). Las ODR, permiten que las partes en un procedimiento de ADR puedan resolver cualquier disputa online de principio a fin. Las ODR eliminan nuestra limitación física, proporcionando un entorno en línea productivo, en el que resolver cualquier tipo conflicto.

Por arbitraje comercial internacional online se entiende aquel que se realiza entre dos o más partes, al momento de la celebración de ese acuerdo, que tienen sus establecimientos, su domicilio o residencia, en diferentes Estados[1013], mediante el empleo de las comunicaciones electrónicas y demás tecnología de la información. La finalidad consiste en solucionar el conflicto, surgido de manera definitiva y en instancia única, mediante la intervención de un tercero independiente o experto, obligándose las partes a cumplir el laudo que se dicte. Se trata de un arbitraje como cualquier otro, en donde se modifica la forma de las actuaciones, dado que se interactúa electrónicamente a través de la plataforma o sala virtual, previamente ofrecida por una institución arbitral y elegida por las partes[1014].

En síntesis, un arbitraje online debe, ante todo, sustentarse en factores tales como el aseguramiento sobre la naturaleza de los datos a transferir, el país de origen, el país receptor, la razón por la cual se procesan los datos y las medidas de seguridad vigentes para la transferencia y el procesamiento de los datos personales en juego.

Internacionalmente, el marco legal del arbitraje es una mezcla de Convenciones internacionales, instrumentos legales, y Leyes nacionales, que regulan tanto su

---

Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52001DC0161 (última visita: 5/5/2014).

[1013] Artículo 1,3 de la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional de 1985, con enmiendas aprobadas en 2006.
Disponible en: http://www.uncitral.org/pdf/spanish/texts/arbitration/ml-arb/07-87001_Ebook.pdf (última visita: 6/5/2014).

[1014] CNUDMI/UNCITRAL: *A/CN.9/WG.III/WP.127 - Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico*, Grupo de Trabajo III (Solución de Controversias en Línea), 29° período de sesiones, Nueva York, 24 a 28 de marzo de 2014, párr.38.
Disponible en:
http://daccess-dds-ny.un.org/doc/UNDOC/LTD/V14/002/80/PDF/V1400280.pdf?OpenElement (última visita: 6/5/2014).

procedimiento como las Leyes de fondo aplicables. Lo que parece estar ocurriendo a distintos niveles, es la modificación del actual régimen de arbitraje internacional, para acomodarlo a las nuevas tecnologías de la información y de las comunicaciones y su aplicación a las formas tradicionales del arbitraje. Sin embargo, a pesar de esta tendencia mundial, para innovar en los sistemas legales nacionales, nos encontramos que, incluso, en el seno de la Unión Europea los regímenes legales son bastante diferentes de un Estado a otro, algunos de los cuales prohíben cualquier sistema que impida a los consumidores llevar sus disputas a un Tribunal tradicional[1015].

En este sentido, muchas de las nuevas normas, que armonizan la legislación internacional sobre el arbitraje comercial internacional, también deben realizarse para las transacciones que se están realizando en el ciberespacio. En la UE ya se han desarrollado marcos legales para tratar de lograr alguna armonización, aunque a través de Directivas, en materias como protecciones de datos, firma electrónica y comercio electrónico, regulando algunos de los problemas legales que se están produciendo en el ciberespacio, sin resolverlo del todo.

Dentro de este contexto de armonización, surgen varias cuestiones legales importantes, dentro de los arbitrajes online, particularmente relativos a la constitución del acuerdo arbitral, el debido proceso y la ejecución de laudos dictados online en los Tribunales estatales. Ante estos problemas jurídicos que se plantean, hay una cuestión fundamental, común a todas ellas[1016], el uso de la firma electrónica, pues ésta garantiza la autenticidad de las comunicaciones, la identidad de las partes y, sobre todo, la identificación de la institución arbitral, que gestiona electrónicamente la causa sometida a arbitraje.

Una vez perfeccionado el acuerdo desplegará dos efectos, uno positivo y otro negativo. El positivo se enmarca en el compromiso que asumen las partes de cumplir con todo lo establecido en el laudo arbitral y colaborar, por ende, en el nombramiento de los árbitros, así como en el desarrollo del procedimiento arbitral. El efecto negativo supone la renuncia de las partes a entablar sus acciones en la jurisdicción ordinaria. Con

[1015] BORGOÑO TORREALBA, J.L.: "Arbitraje Comercial Internacional online", *Anuario Español de Derecho Internacional (AEID)*, 2007, núm. 23, págs. 247-278.
[1016] ETEL RAPALLINI, L.: "La empresa y el arbitraje "on line" en el comercio internacional", *Derecho Internacional,* ANALES Nº 42 - Facultad de Cs. Jurídicas y Sociales. U.n.l.p. 2012, págs. 172-181.

todo, se puede plantear dificultades en la identificación de las partes involucradas a través de la firma electrónica y, a la vez, dificultades a la hora de garantizar la autenticidad del convenio arbitral; es decir, acreditar su existencia y plena validez con el objetivo de que produzca todos sus efectos.

En este contexto, toma importancia: el principio de equivalencia funcional entre el documento con soporte papel y el documento electrónico, entre la firma autógrafa y la firma electrónica; el principio de neutralidad tecnológica, estableciéndose un parámetro de igualdad entre el mecanismo presencial y el virtual; y el principio de confianza mutua y su reflejo en el de buena fe.

En todo caso, los textos internacionales y nacionales requieren que la libre decisión de las partes conste de forma indubitada. De ahí que, se requiera que el convenio arbitral conste "por escrito". No se trata de un requisito de pura formalidad que se agota en sí mismo. Se exige, como primer paso, que haya una manifestación de voluntad fácilmente accesible, para conocer la voluntad de las partes y el alcance de ésta. Luego vendrá la determinación del contenido de la cláusula arbitral, que señala el ámbito o límites de la actuación arbitral; pues, el primer paso en pro de la electronificación, se da por parte del regulador al admitir, expresamente, que la constancia escrita del convenio arbitral, no se circunscribe al soporte papel, sino que abarca también el soporte electrónico[1017].

En cualquier caso, el debate sobre la validez del convenio arbitral, perfeccionado por medios electrónicos se plantea como consecuencia de los requisitos de forma exigidos por la Convención sobre Reconocimiento y Ejecución de Sentencias Arbitrales Extranjeras (Nueva York el 10 de junio de 1958), que por un lado, el Artículo 2 exige que el acuerdo conste por escrito y firmado por las partes, a no ser que resulte contenido en un canje de cartas o telegramas; y por otro, el Artículo 4, a efectos de reconocimiento y ejecución, obliga a las parte ejecutante a presentar el acuerdo arbitral original o copia que reúna las condiciones requeridas para su autenticidad, lo que genera problemas de consentimiento de las partes al arbitraje.

[1017] MADRID PARRA, A.: "Electronificación del arbitraje", *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Riedpa)*, 2011, núm. 2.
Disponible en: http://www.riedpa.com/COMU/documentos/RIEDPA21103.pdf (última visita: 6/6/2014).

La Convención de Nueva York no admite expresamente el canje de e-mails u otro tipo de comunicaciones electrónicas. Sin embargo, esta realidad fáctica si ha sido contemplada por el Artículo 7,2 de la Ley Modelo de la CNUDMI/UNCITRAL sobre Arbitraje Comercial Internacional al aceptar el télex, telegramas u "otros medios de telecomunicación que dejen constancia del acuerdo". Aquí se pone de manifiesto esa posición abierta a la recepción de toda innovación, que facilite la contratación y la resolución de conflictos de intereses, y el Artículo 6,1 de la Ley Modelo sobre Comercio Electrónico dispone: "cuando la Ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta". Asimismo, el Artículo 2 nos dice que se entenderá "por mensaje de datos: la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax". La expresión, que indica el requisito necesario para que se aplique el principio de equivalencia funcional a "escrito"; esto es, que la información esté "accesible para su ulterior consulta", ha sido incorporada a distintos ordenamientos jurídicos que han seguido la pauta de la Ley Modelo al contemplar la validez jurídica de la información existente en soporte electrónico[1018], especialmente, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005), que en el Artículo 9,2 dice: "cuando la ley requiera que una comunicación o un contrato conste por escrito, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta", observándose que su Artículo 20,1 dispone la posibilidad de que las disposiciones de la Convención serán aplicables al empleo de comunicaciones electrónicas en lo concerniente a la formación o el cumplimiento de un contrato al que sea aplicable cualquiera de los siguientes instrumentos internacionales, en los que un Estado contratante de la presente Convención sea o pueda llegar a ser parte de: Convención sobre el Reconocimiento y Ejecución de las Sentencias Arbitrales Extranjeras (Nueva York, 10 de junio de 1958); Convención sobre la Prescripción en Materia de

[1018] MADRID PARRA, A.: "Electronificación del arbitraje", *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Riedpa)*, 2011, núm. 2.
Disponible: http://www.riedpa.com/COMU/documentos/RIEDPA21103.pdf (última visita: 6/6/2014).

Compraventa Internacional de Mercaderías (Nueva York, 14 de junio de 1974) y su Protocolo (Viena, 11 de abril de 1980); Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 11 de abril de 1980); Convenio de las Naciones Unidas sobre la Responsabilidad de los Empresarios de Terminales de Transporte en el Comercio Internacional (Viena, 19 de abril de 1991); Convención de las Naciones Unidas sobre Garantías Independientes y Cartas de Crédito Contingente (Nueva York, 11 de diciembre de 1995); Convención de las Naciones Unidas sobre la Cesión de Créditos en el Comercio Internacional (Nueva York, 12 de diciembre de 2001).

Consecuencia de esta realidad es la puesta a disposición de los Estados de la Convención de las Naciones Unidas para que dicho fenómeno de electronificación se incorpore a Convenciones ya existentes sin necesidad de una modificación formal de las mismas, como ya comentamos en Capítulo anterior.

Sin embargo, a día de hoy, si bien se observa una tendencia a favor del arbitraje mercantil internacional online, a la vez que se ha establecido una regulación clara de la firma electrónica, a la que se le asigna igual eficacia jurídica que la firma manuscrita, no se ha producido una adecuación plena entre las legislaciones respecto de los avances tecnológicos, sin que exista ese criterio de reciprocidad requerido internacionalmente entre los Estados.

Así, cuando lo habitual es que el acuerdo de arbitraje se encuentre en un contrato físicamente firmado por las partes; en este caso no hay ninguna duda, en un principio, que la cláusula arbitral es válida y obligatoria para las partes. Sin embargo, en el caso del comercio internacional el problema que surge es que, habitualmente, no se firman contratos físicamente, sino que se procede de manera informal, materializada, muchas veces, en órdenes de compra enviadas por fax o por e- mail. Además, existe el dilema de saber si el acuerdo arbitral suscrito por medios electrónicos (por ejemplo, a través de intercambio de correos electrónicos o prestando el consentimiento a través de un sitio Web) es suficiente para invocar su validez y ejecutabilidad. En cualquier caso, al respecto, habrá que tener en cuenta la regulación existente en cada uno de los Estados sobre firma electrónica, con todos lo ya planteado.

Por ello, considerando el tenor arbitrable de las disputas, basado en un acuerdo de arbitraje voluntario, que no será considerado válido si las materias que forman parte del acuerdo no son arbitrables; esto es, si las partes no disponen del poder de disposición de dichas materias, de igual forma la puesta en marcha de una modalidad no presencial, deberá contar con el acuerdo de las partes y sobre ésta expectativa, sumado a la protección de datos que se transfieran, resulta una oferta tentadora de ser captada por las instituciones arbitrales, por los profesionales y por los particulares que reciban su asistencia. Así pues, los procedimientos de resolución de litigios en línea no está actualmente suficientemente desarrollados, tal como ha reconocido la Comisión Europea[1019]; pues, nos encontramos que los aspectos transfronterizos, de los problemas identificados en la resolución de litigios en línea, están directamente relacionados con la situación nacional[1020].

6.4.5. Consideraciones finales

La proyección internacional de la firma electrónica supone que haya que adoptar una fórmula válida para todos los ordenamientos jurídicos nacionales, que les permita englobar jurídicamente las posibles diferencias existentes en los ordenamientos jurídicos ante la falta de estándares y/o protocolos de actuación uniforme, por la ausencia de control técnico y legal de todos los aspectos del comercio electrónico, especialmente, de la firma electrónica.

Lo que plantea mayor dificultad es determinar que la jurisdicción, internacionalmente, es competente a la transacción que se realiza, surgiendo una obligación entre personas situadas en lugares diferentes, donde el elemento internacional de la obligación que subyace debería obligar a determina que: la necesidad de que el derecho que resulte aplicable sea el que tenga una mayor cercanía o una mayor fuerza probatoria fidedigna.

[1019] Considerando 6 de la Directiva 2013/11/UE del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) nº 2006/2004 y la Directiva 2009/22/CE (Directiva sobre resolución alternativa de litigios en materia de consumo).

[1020] COMISIÓN EUROPEA: *Documento de trabajo de los servicios de la comisión resumen de la evaluación del impacto que acompaña a los documentos Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la resolución alternativa de litigios en materia de consumo (Directiva sobre RAL en materia de consumo), (SEC(2011) 1409 final),* Bruselas, 29 de noviembre de 2011, pág. 4.

La aplicación de *fórum non conveniens* puede suponer una posibilidad a la remodelación del modelo en formato papel o físico hacia la adecuación del modelo tecnológico. El motivo, que nos lleva a esta conclusión, es la existencia de reciprocidad previa existente en los litigios entre el comercio internacional y el Derecho que lo regula; pues, de lo que se trata es de permitir extender la jurisdicción personal sobre quienes hacen gestiones de negocios desde otro Estado, de tal manera que el Estado que tenga vínculos más estrechos con el asunto sea quien decida sobre el éste.

Esto lleva realizar una necesaria diferenciación; por un lado, la ley aplicable al procedimiento, determinando que foro es más idóneo para resolver sobre el asunto, prestando atención a cuál es el foro en que se pueden tener elementos probatorios que permitan dar una mejor solución al conflicto surgido; y por otro, el Derecho aplicable al contrato litigioso, que vendrá a determinar las cuestiones del fondo relativas al contrato, que se haya celebrado por vía electrónica, que afectará a su existencia y validez, interpretación, cumplimiento e incumplimiento de derechos y obligaciones, extinción y la nulidad del mismo.

Esta solución de controversias podría extenderse a las Online Dispute Resolution (ODR), cuyo mecanismo más formal es el arbitraje. Las ODR tienen la ventaja de permitir elegir el o los árbitros, la Ley aplicable al procedimiento arbitral y a la decisión de la controversia, así como la posibilidad de que la sentencia arbitral o laudo no esté sujeto a apelaciones. Además, el cumplimiento forzoso del laudo se ve facilitado internacionalmente en alguno de los 142 Estados que han ratificado la Convención de Nueva York.

Sin embargo, como hemos visto, barreras jurídicas y técnicas obstaculizan la tramitación integra del arbitraje por medios electrónicos o telemáticos, que lastran su desarrollo. El debate lo centramos principalmente:

a) De un lado, la Ley aplicable que, en virtud de la autonomía voluntad, puede ser escogida por las partes. Si las Partes no han determinado el Derecho aplicable al convenio arbitral, éste podrá ser establecido por los árbitros. No obstante, esta situación no ha sido expresamente reconocida por los distintos

Convenios internacionales, reglamentos de arbitraje ni por las distintas legislaciones nacionales, bien es sabido que es aceptado internacionalmente que el Tribunal arbitral es competente, para resolver todas las cuestiones relativas a su propia competencia y cuando lo haga, necesariamente, deberá pronunciarse acerca del Derecho que consideró aplicable al convenio arbitral[1021]. De esta forma, las dudas acerca de las leyes aplicables al arbitraje se convierte en una preocupación primordial para el comercio internacional.

b) De otro, el procedimiento con respecto:

   a. Al contenido en un canje de cartas o telegramas (Artículo 2 de la Convención de Nueva York de 1958). Respecto a esta cuestión, el artículo 7,2 de la Ley Modelo sobre Arbitraje Comercial Internacional de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL) declara que "el requisito de forma escrita se cumple si el convenio de arbitraje está en un documento firmado por las partes o en otros medios de telecomunicaciones que proporcionen un registro de dicho acuerdo"[1022].

   b. A la obligación de la parte ejecutante, que debe presentar el acuerdo arbitral original o copia que reúna las condiciones requeridas para su autenticidad (Artículo 4 de la Convención de Nueva York de 1958), generando la problemática en la prueba del consentimiento. Cuando los procedimientos se desarrollan online pueden surgir dificultades si la normativa aplicable depende de la localización física. Esto puede conducir a lo que la doctrina denomina "laudo flotante" (*floating award*) o "arbitraje flotante" (*floating arbitration*), pudiendo llegar a repercutir en importantes cuestiones.

[1021] BORGOÑO TORREALBA, J.L.: "Arbitraje Comercial Internacional online", *Anuario Español de Derecho Internacional (AEID)*, 2007, núm. 23, págs. 247-278.
[1022] Esta interpretación ha sido, en principio, respaldada por el Artículo 17 de la Directiva sobre comercio electrónico y el Reglamento 910/2014 sobre identificación electrónica.

Finalmente, la Unión Europea, dada la creciente importancia del comercio en línea y, en particular, del comercio transfronterizo como pilar de la actividad económica de la Unión, ha considerado necesario contar con una infraestructura para la resolución alternativa de litigios, en materia de consumo, que funcione correctamente y con un marco para la resolución de litigios en línea, respecto a los consumidores, ante la existencia de normas internas en cada Estado miembro que establecían prescripciones tasadas en distintos ámbitos que evidenciaban deficiencias y restaban efectividad a la resolución de conflictos.

Ante esta situación el 18 de junio de 2013, se adoptaron simultáneamente dos marcos normativos complementarios de referencia para el arbitraje online de consumo y que vienen a establecer soluciones a los problemas planteados anteriormente: la Directiva 2013/11/UE[1023] relativa a la resolución alternativa de litigios en materia de consumo por la que se modifica el Reglamento (CE) nº 2006/2004[1024] y la Directiva 2009/22/CE y el Reglamento 524/2013 sobre resolución de litigios en línea en materia de consumo[1025].

Con estas normas se plantean soluciones a las cuestiones suscitadas anteriormente, aunque como decimos solo en materia de consumo. Respecto a la Ley aplicable, en los procedimientos que tengan por objeto resolver un conflicto, mediante la imposición de una solución, cuando no exista conflicto de leyes, la solución impuesta no podrá privar al consumidor de la protección que le proporcione la normativa imperativa del Estado miembro, en que el consumidor y el comerciante tengan su residencia habitual; cuando exista conflicto de leyes y la ley aplicable se determine con arreglo al Artículo 6, apartados 1 y 2 del Reglamento nº 593/2008 o al Artículo 5, apartados 1 a 3, del Convenio de Roma de 19 de junio de 1980 sobre la Ley aplicable a las obligaciones contractuales[1026].

[1023] Plazo de incorporación de la Directiva al Derecho nacional se extiende hasta el 9 de julio de 2015.
[1024] Aplicable a partir del 9 de enero de 2016.
[1025] MADRID PARRA, A.: "Directiva 2013/11 (ADR) y Reglamento 524/2013 (ODR): Una apuesta europea por la solución alternativa de litigios y en pro del comercio electrónico transfronterizo", *Spain Arbitration Review. Revista del Club Español del Arbitraje*, nº. 18, 2013, p. 37-62.
[1026] El considerando 5 de la Directiva 2013/11/UE, relativa a la resolución alternativa de litigios en materia de consumo, nos dice que: "la solución impuesta por la entidad de resolución alternativa no pueda dar lugar a que el consumidor se vea privado de la protección ofrecida por disposiciones que no

Por otro lado, en relación con el procedimiento, el contenido esencial de la Directiva va referido al establecimiento de requisitos que deben cumplir las entidades de resolución alternativa de litigios; el acceso de los consumidores a tales entidades; las condiciones que deben reunir las personas físicas encargadas de la resolución alternativas de litigios (conocimientos especializados, independencia e imparcialidad); las obligaciones de transparencia de dichas entidades; la eficacia de los diversos tipos de procedimientos; el régimen jurídico aplicable en tales procedimientos; la información y asistencia a los consumidores en este ámbito; la cooperación entre entidades de resolución y entre estas y las autoridades nacionales competentes; así como las funciones de dichas autoridades y de la Comisión. Además, el Reglamento crea una plataforma de resolución de litigios en línea en el ámbito de la Unión, facilitando un cauce de resolución extrajudicial de litigios entre consumidores y comerciantes. De esta manera, se podría decir, que al establecerse estas normas con el fin de dar soluciones a conflictos establecidos, de manera armonizada, a través del desarrollo de un nuevo marco para el comercio internacional, aunque solo sea en materia de consumo, sirven de base para el establecimiento de la tramitación integra del arbitraje a través de medios telemáticos.

puedan excluirse mediante acuerdo en virtud de la ley del Estado miembro en que el consumidor tenga su residencia habitual" (o el estándar equivalente del Convenio de Roma de 1980 "si la ley aplicable al contrato de compraventa o de servicios se determina con arreglo al artículo 5, apartados 1 a 3" de dicho Convenio) (como es conocido, el Reglamento Roma I se aplica a los contratos celebrados a partir del 17 de diciembre de 2009).

CONCLUSIONES

1ª.- Hoy día, podemos decir que Internet es la máxima expresión del comercio internacional, donde se producen nuevas formas de comunicación, información y comercialización. Ante esta situación resulta necesaria la introducción de normas, en los ordenamientos jurídicos existentes, observando el propio fenómeno tecnológico, el cual se está desarrollando y dando una respuesta global y armonizada, para resolver cualquier problema e incertidumbres que pueda plantearse.

2ª.- De resolver cualquier problema e incertidumbre se ha tratado de ocupar la CNUDMI/UNCITRAL con sus Leyes Modelo sobre Comercio Electrónico y Firma Electrónica y la Convención sobre Utilización de las Comunicaciones Electrónica en los Contratos Internacionales. Sin embargo, si bien sus normas han inspirado a todos los Estados, que han desarrollado Leyes en estas materias, no han logrado el objetivo perseguido: armonización legislativa internacional.

Cada Estado ha desarrollado normas divergentes constituyendo un entorno que, en cierta medida, ha creado nuevas barreras al comercio electrónico internacional, creando incertidumbres en torno a la firma electrónica, en cuanto a: sus funciones elementales, formas, requisitos legales, su valor jurídico y responsabilidad entre las partes participantes, en el marco de las transacciones de carácter transfronterizo. Lo que ha constituido un serio obstáculo para el desarrollo de un marco armonizado internacional.

3ª.- Deliberadamente, hemos partido de la definición de firma electrónica dada en los textos de la CNUDMI, centrándonos en la recogida por la Ley Modelo sobre Firma electrónica, que ha servido de guía a todos los Estados.

En esta definición se aprecian las tres funciones o elementos de los que consta la firma electrónica: identidad (¿quién es usted?), autenticación de la identidad (¿cómo puede probarlo?) y autorización o autenticación de la transacción (¿a qué está usted autorizado?). La mayoría de las Leyes nacionales se han centrado en esta última función.

4ª.- Del análisis realizado, se observa, con respecto a las cuestiones de identidad y la idoneidad del método de identificación de las partes, que no ha habido un pronunciamiento internacional que sirva referencia, ni siquiera las Leyes Modelo de la CNUDMI se han ocupado de cuestiones relacionadas con la validez o la verificación de la identidad. Salvo el Reglamento 910/2014 aprobado, relativo a la identificación electrónica, que presenta soluciones de gestión de la identidad, en el contexto de la gobernanza electrónica dentro de la Unión Europea.

5ª- Las legislaciones de muchos Estados presentan procesos de validez y verificación propios, centrándose en la emisión de credenciales nacionales, a través de entes de naturaleza pública. Se trata de procesos que conllevan la emisión de dispositivos (tarjetas del ciudadano, eDNI, etc.) que, entre otras cosas, les permiten utilizar firmas electrónicas a bajo costo. Aunque el objetivo principal de estas iniciativas no es comercial, estos mecanismos pueden utilizarse en este ámbito, reconociéndose la convergencia de los dos ámbitos de aplicación: público y privado.

Se aprecia que al ser la emisión de credenciales gestionada por un Estado, dentro de su propio sistema nacional en exclusividad, a través de Leyes con naturaleza jurídica pública o administrativa, centrándose la expedición de la misma en una autoridad nacional, se confirma la identidad de modo que, posteriormente, sólo es demostrable dentro del sistema nacional propio. De esta forma, el reconocimiento de los servicios de autenticación de identidad extranjeros se presenta muy complicado ante una labor centrada en el establecimiento de servicios nacionales.

6ª.- Pueden surgir complicaciones con respecto a la aceptación de credenciales, que suele darse en el uso transfronterizo de documentos firmados con la intervención de alguna autoridad pública; pues, las autoridades receptoras de un país extranjero suelen exigir alguna prueba de la identidad y autoridad del firmante. Por tradición, esos requisitos se cumplen por los procedimientos de “legalización”, a través de la denominada Apostilla Electrónica, en los que las firmas que figuren en documentos nacionales son autenticadas por las autoridades diplomáticas para su utilización en el extranjero, sin que aún haya un funcionamiento efectivo total.

7ª.- Se observan dificultades en los sistemas de gestión relacionadas con la esfera privada de los riesgos, que entraña la utilización indebida de identificadores exclusivos: pueden plantearse problemas por las diferencias en las normas vigentes, en particular, con respecto a la posibilidad de delegar la facultad de actuar en nombre de otra persona: se ponen soluciones basadas en la cooperación empresarial voluntaria; sin embargo, este enfoque no basta para reglamentar todas las cuestiones conexas y requiere de la adopción de un marco jurídico.

8ª.- Del estudio realizado de los procesos de autenticación o autorización de la transacción se aprecian diferencias sustanciales de un ordenamiento jurídico a otro. Estos procesos se relacionan con los actos conexos de autenticación y firma, que poseen funciones que no tienen por qué corresponderse propiamente con el propósito y la función de los métodos electrónicos de firma y autenticación. En ocasiones se utiliza la palabra autenticación de forma genérica en relación con el aseguramiento de la autoría y la integridad de la información de la información, pero cabe la posibilidad de que algunos ordenamientos jurídicos establezcan distinciones entre esos elementos. Por ello, podemos decir que las nociones de firma y autenticación no son objeto de una interpretación uniforme, sino que las funciones que cumplen son distintas de un sistema jurídico a otro.

Todo va a depender del reconocimiento legal de la firma electrónica y de las presunciones de validez y eficacia, que se dé a los documentos autenticados con determinados tipos de firma electrónica. Ante el riesgo de manipulación de los documentos electrónicos, muchos países dejan al arbitrio de los Tribunales el valor probatorio de la firma electrónica más simple, insertada; por ejemplo, en correos electrónicos, debiendo las actuaciones judiciales establecer si garantizan o no, suficientemente, su integridad.

9ª- Una amplia variedad de métodos para autenticar o autorizar una transacción electrónica, desde el uso de contraseñas hasta firmas digitales, firmas biométricas, etc. A la hora de reglamentar su uso, las Leyes deberían prestar atención a la flexibilidad suficiente, para abarcar todas las tecnologías posibles; pues, centrarse en una tecnología específica puede obstaculizar la utilización de otras tecnologías. Esto se facilitaría mediante disposiciones neutrales tecnológicamente hablando.

Sin embargo, las Leyes se debaten entre la fiabilidad y la confianza/seguridad convirtiendo el uso transfronterizo de la firmas electrónicas en un verdadero problema en los sistemas que dan preferencia a una tecnología determinada. La complejidad aumenta en proporción directa al grado de regulación estatal de las firmas y autenticación electrónicas y al grado de seguridad jurídica que la Ley concede.

10ª.- Fundamentándose en la seguridad, la legislación interna que da preferencia a una tecnología determinada, principalmente, a una infraestructura de clave pública, debería permitir reconocer íntegramente otras firmas basadas en la misma tecnología. Sin embargo, se produce el establecimiento de requisitos añadidos, que se refieren, de manera expresa, al reconocimiento de certificados extranjero, a la vez que imponen una carga suplementaria al prestador de servicios de certificación extranjero. Tratando de examinar: su equivalencia jurídica, equivalencia en las obligaciones legales y la equivalencia en los regímenes de responsabilidad. Esto nos permite hablar, en la práctica, de sistemas cerrados, no solo porque los titulares de los certificados están ya estrechamente vinculados por reglas ya preestablecidas, sino que, además, las Leyes de firma electrónica varían conceptos, incluso en el trato de la misma tecnología, que se detectan, principalmente, en las disposiciones detalladas respecto a la naturaleza y la fiabilidad y/o seguridad de la firma electrónica, las conductas de las partes y el reconocimiento transfronterizo de las firmas electrónicas y sus certificados, situándonos ante la falta de interoperabilidad jurídica, a la que hay que sumarle la interoperabilidad técnica como agravante.

11ª.- Las cuestiones de responsabilidad son una preocupación fundamental; pues, todos los participantes en una transacción tienen que saber quién asumirá la responsabilidad asociada a la reparación de cualquier daño que pudiera causarse en la propia transacción, en relación con el uso de la firma electrónica. La base jurídica que sustentan los procesos de certificación, aplicabilidad del proceso de certificación, la asignación del riesgo y la responsabilidad de los usuarios, prestadores y terceros no se han prestado a la armonización a nivel internacional.

La preocupación resulta de las diferencias existentes entre los regímenes de responsabilidad de los diversos países y los elementos comunes a todos ellos, de modo

que dificultan los métodos y procedimientos apropiados para reconocer las firmas respaldadas por certificados extranjeros. Con frecuencia los mecanismos que establecen la responsabilidad de las partes no están bien definidos y son inciertos, presentándose una barrera básica para el sector privado a la hora de adoptar soluciones interoperables.

12ª.- Se observan problemas sobre cuestiones relativas a la aplicación de Leyes y reglamentaciones en relación con la jurisdicción competente, que resulta de la transacción que se produce entre personas situadas en lugares diferentes, donde el elemento internacional de la obligación, que subyace, obliga a determinar qué Derecho resulta aplicable, sea el que tenga una mayor cercanía o sea el que tenga una mayor fuerza probatoria fidedigna. Cuando se presenta un elemento extranjero, en una situación jurídica, se complica la respuesta práctica a la misma, ya sea ésta judicial o extrajudicial, por concurrir en ella distintos intereses y por hallarse vinculada con diferentes ordenamientos jurídicos; pues, la mayoría de los sistemas jurídicos se basan en el principio de que los Estados soberanos ejercen jurisdicción exclusiva dentro de su propio territorio, lo que nos ha llevado a la extraterritorialidad de la jurisdicción.

LEGISLACIÓN

Alemania:

- Gesetz zur digitalen Signatur (Signaturgesetz - SigG) (22 de julio de 1997).
- Gesetz über Rahmenbedingungen fürelektronische Signaturen (Signaturgesetz - SigG). (16 de Mayo de 2001).

Australia:

- AUSTRALIA: Electronic Transactions Act (Act No. 162 of 1999) modificada por la Electronic Transactions Amendment Act (2011).
- Electronic Transaction Act de 2000 (Nueva Gales del Sur).
- Electronic Transactions de 2000 (Queensland).
- Electronic Transactions Act de 2000 (Australia Meridional).
- Electronic Transactions Act de 2000 (Tasmania).
- Electronic Transactions de 2000 (Victoria).
- Electronic Transactionsde 2000 (Territorio del Norte).
- Electronic Transactions Act de 2001 (Territorio de la Capital Australiana).
- Electronic Transactions Act de 2003 (Australia Occidental).

Argentina:

- Ley 25.506 sobre Documento Electrónico y Firma Digital (2001).

Chile:

- Ley Nº 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firmas Electrónicas (2002).

China:

- Contract Law of the People's Republic of China (Adoptada y promulgada el 15 de marzo 1999).
- Electronic Signature Law of the People's Republic of China.
- Certification Authority Regulations (2005).

CNUDMI/UNCITRAL:

- Convención sobre Reconocimiento y Ejecución de Sentencias Arbitrales Extranjeras (Nueva York el 10 de junio de 1958).
- Convenio de Viena de los Tratados de 1969.
- Convención de Viena de 1980 sobre los Contratos de Compraventa Internacional de Mercaderías.
- Ley Modelo de la CNUDMI/UNCITRAL sobre Arbitraje Comercial Internacional (de 1985, con enmiendas adoptadas en 2006).
- Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). Fecha de adopción: 12 de junio de 1996 (el artículo 5 bis suplementario fue adoptado en 1998).
- Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). Fecha de adopción: 5 de julio de 2001.
- Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005). Fecha de adopción: 23 de noviembre de 2005.

Conferencia de La Haya:

- Convenio de La Haya de 5 de octubre de 1961sobre la Suprimiendo la Exigencia de Legalización de Documentos Públicos Extranjeros.
- Convenio de La Haya de 2005 sobre Acuerdos de Elección del Foro.

España:

- Real Decreto de 24 de julio de 1889 por el que se dispone la publicación del Código civil.
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD).
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos, para la sustitución de la aportación de certificados por los ciudadanos.
- Real Decreto 1533/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.
- Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior relativa a los certificados de firma electrónica, incorporados al Documento Nacional de Identidad.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 56/2007, de 28 de diciembre de 2007, de medidas de impulso de la Sociedad de la Información..
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

Estados Unidos:

- Utah Digital Signature Act Utah.Code §§ 46-3-101 to 46-3-504. (Promulgada en 1995).
- Uniform Electronic Transaction Act (UETA, julio de 1999)
- Electronic Signature in Global and Nacional Commerce Act (E-SIGN, 30 de julio de 2000).
- REAL ID Act 2005.

Italia:

- Legge n. 59/1997 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa" (17 marzo 1997).
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445: "Disposizioni legislative in materia di documentazione amministrativa. (Testo A)."
- Decreto Legislativo 23 gennaio 2002, n. 10: "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche".
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali".
- Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale".

Reino Unido:

- Statute of Frauds (1677)

- Electronic Communications Act (2000).
- The Electronic Signatures Regulations (2002).

Singapur:

- Electronic Transactions Act (1998).
- Electronic Transactions Act (2010).

Unión Europea:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
- Reglamento 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
- Convenio de Bruselas de 1968 relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil.
- Convenio de Roma de 19 de junio de 1980 sobre la Ley aplicable a las obligaciones contractuales.
- Directiva 115/2001/CE del Parlamento Europeo y del Consejo, de 20 de diciembre, por la que se modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el Impuesto sobre el Valor Añadido.

- Directiva 2006/112/CE del Parlamento Europeo y del Consejo, relativa al sistema común del impuesto sobre el valor añadido.
- Directiva 2010/45/UE del Consejo de 13 de julio de 2010 por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a las normas de facturación.
- Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006, relativa a los servicios en el mercado interior.
- Tratado de Lisboa de 13 de diciembre de 2007.
- Tratado de Funcionamiento de la Unión Europea (C83/47 – 30, de 30 marzo de 2010).
- Reglamento 593/2008, de 17 de junio de 2008, sobre la Ley aplicable a las obligaciones contractuales (Roma I).
- Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011 sobre los derechos de los consumidores.
- Reglamento 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
- Directiva 2013/11/UE del Parlamento Europeo y del Consejo, relativa a la resolución alternativa de litigios en materia de consumo por la que se modifica el Reglamento (CE) nº 2006/2004 y la Directiva 2009/22/CE.
- Reglamento 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo.
- Reglamento Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por el que se deroga la Directiva 1999/93/CE sobre firma electrónica.

SENTENCIAS

Alemania:

- Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 de abril de 2000, JurPC Internet- für Zeitschrift Rechtsinformatik und Informationsrecht, JurPC Web-Dok. Nº 160/2000.
- Sentencia del Tribunal de AG Ettlingen de 11 de mayo de 2001, Caso Nº 2 C 259/00.
- Sentencia del Tribunal de AG Bonn de 25 de octubre de 2001**,** número de caso 3 C 193/01.
- Sentencia del Tribunal Superior de Colonia, de 6 de septiembre de 2002, número de caso 19 U 16/02.
- Sentencia del Tribunal superior Administrativo de Rhineland-Palatinate (OVG Rheinland-Pfalz), de 21de abril de 2006.

Australia:

- R. v. Moore: ex part Myers (1884) 10 V.L.R.
- R v Frolchenko (1998) QCA 043.
- Cloud Corp. v. Hasbro Inc., 314 F.3d 289 (2002).
- Caso Gutnick v Dow Jones & Co Inc. [2002] HCA 56; (2002).
- Pretty Pictures Sarl v Quixote Films Ltd" 16 [2003] All ER (D) 303 (Jan).
- McGuren v Simpson [2004] NSWSC 35 (18 de febrero 2004).
- Olivaylle Pty Ltd v Flottweg GMBH & Co KGAA (No 4) [2009] FCA 522 (20 May 2009).

Colombia:

- Sentencia de la Corte Constitucional C-662 del 8 de junio de 2000, de 8 de junio de 2000 (Expediente D-2693).

Eslovenia:

- Corte Suprema de la Republica de Eslovenia (caso I UP 505/2003), 18 de junio de 2003.

España:

- Sentencia del Tribunal Supremo de 25 de enero de 1989.
- Sentencia del Tribunal Supremo en Sentencia de 1 de marzo de 1993.
- Sentencia del Tribunal Supremo (Sala de lo Civil) núm. 677/1994, de 9 julio (RJ 1994\6302).
- Sentencia del Tribunal Supremo (Contencioso-Administrativo) de 3 noviembre 1997 (RJ 1997\8251).
- RESOLUCIÓN de 11 de junio de 1999, de la Dirección General de los Registros y del Notariado, en el recurso gubernativo interpuesto por el Notario de Torroella de Montgrí, don Leopoldo de Urquía y Gómez contra la negativa de la Registradora de la Propiedad de Bisbal d'Empordá, doña Raquel Laguillo Menéndez-Tolosa, a inscribir una escritura de compraventa, en virtud de apelación del recurrente (BOE núm. 166, Martes 13 julio 1999.
- Sentencia del Tribunal Constitucional de 292/2000, de 30 de noviembre de 2000 (RTC 2000\292).
- Sentencia Audiencia Nacional (Contencioso-Administrativo) de 15 enero 2011 (RJCA 2011\2).
- Sentencia Tribunal Supremo de 15 de junio de 2011.
- Sentencia de la Audiencia Provincial de Barcelona de 21 de junio de 2011.
- Sentencia del Tribunal Supremo de 27 junio de 2011.

- Sentencia del Tribunal Supremo, número 756/2012, de 13 de diciembre (RJ 2013/1250).
- Sentencia de la Audiencia Provincial de Madrid de 31 de mayo de 2013.

Estados Unidos:

- International Shoe v. Washington, 326 U.S. 310 (1945).
- Gulf Oil Corp. v. Gilbert - 330 U.S. 501 (1947).
- McGee v. International Life Insurance Co., 355 U.S. 220 (1957).
- Piper Aircraft Co. v Reyno - 454 EE.UU 235 (1981).
- Re a Debtor (Nº. 2021 de 1995) [1996] 2 All E.R. 345 a 351.
- Zippo Fabr. Co. v Zippo Dot Com, Inc., 952 F. Supp. 1119 (1997).
- Doherty v. Registry of Motor Vehicles No. 97 CV 0050 (1997).
- Shattuck v. Klotzbach, 14 Mass. L. Rep. 360 (Super. Ct., Mass., December 11, 2001).
- Rosenfeld v. Zerneck, 4 Misc. 3d 193, 776 N.Y.S.2d 458 (Sup. Ct., Kings Co. 2004).
- In Re Vee Vinhnee, 336 B.R. 437 (9th Cir. BAP (Cal.) 2005).
- Vista Developers Corp. V. VFP Realty LLC, 2007, NY Slip Op 27418 (17 Misc. 3d 914) Supreme Court, Queens County, October 8, 2007.
- Lorraine v. Markel American Ins. Co. 241 F.R.D. 534, 538 (d. Md. 2007).

Francia:

- Resolución del Consejo de Estado N º 88665 (de 8 de julio de 1988, Bernhard Dietschi).
- Resolución del Consejo de Estado N º 112949 (de 13 de marzo 1996 Diraison).
- Sentencia de la Corte de Casación, juzgado de lo civil, caso "Société Chalets Boisson v MX" (Número 00-46467), de fecha 30 de abril 2003.

- Sentencia del Tribunal de Apelaciones de Nancy, núm. 442/12, de 14 de febrero de 2013.

Italia:

- Tribunale Mondovi, 7 giugno 2004, n. 375.
- Tribunal de Catanzaro, Sentencia de 23 de abril de 2012.

Puerto Rico:

- Sentencia la Corte Suprema de Puerto Rico de 6 de octubre de 2009 (Caso nº: CC-2005-553).

Reino Unido:

- Jenkins v Gaisford y Thring (1863) 3 Sw & T 93.
- Bennet v Brumfitt (1867-1868) 3 LRCP 28.
- Godwin v Francis (1870) LR 5 CP 295.
- Goodman v J Eban ltd (J) Ltd [1954] 1 All ER 763.
- Newborne v Sensolid (Gran Bretaña) LD [1954] 1 QB 45.
- Steadman v Steadman [1976] AC 536 (" Steadman").
- Mehta v J Pereira Fernandes SA [2006] EWHC 813 (Ch).

Singapur:

- SM Integrado Transware Pte Ltd v Schenker Singapur (Pte.) Ltd. [2005] SGHC 58, de 20 de marzo de 2005.
- Wee Soon Kim Anthony v Lim Chor Pee y Otros [2005] 4 SRL 367; [2005] SGHC 159, de 30 de Agosto de 2005.
- Joseph Mathew y Otro v Singh Chiranjeev (y Otro [2009] ASGC 51, de fecha de 29 de octubre de 2009).

Unión Europea:

- Sentencia del Tribunal de Justicia de la Unión Europea de 28 de septiembre de 1999 (GIE Groupe Concorde y otros, C440/97).
- Sentencia del Tribunal de Justicia de la Unión Europea de 9 de diciembre de 2003 (Gasser, C116/02).
- Sentencia del Tribunal de Justicia de la Unión Europea de 25 de octubre de 2011 (eDate Advertising GmbH vs Olivier Martinez, Robert Martinez y MGN Limited, asuntos acumulados C-509/09 y C-161/10).
- Sentencia del Tribunal de Justicia de la Unión Europea de 12 de mayo de 2011 (BVG vs. JPMorgan Chase Bank NA, Frankfurt Branch, C-144/10)
- Sentencia del Tribunal de Justicia de la Unión Europea de 23 de abril de 2009 (Falco Privatstiftung y Rabitsch, C-533/07).

BIBLIOGRAFÍA

- ABA IDENTITY MANAGEMENT LEGAL TASK FORCE: *Meeting report ABA Identity Management Legal Task Force*, Londres, 10 – 11 diciembre, 2012.
- ABA: *Assessment Guidelines: guidelines to help assess and facilitate interoperable trustworthy public key infrastructures*, Chicago, mayo 2003.
- ABA: *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, Chicago, 1996.
- ADAM, J.: "Electroniche Signatur und eropäisches Privatech", *Zeitschrift für europäiches Privatech*, 2001.
- ALAMILLO DOGINGO, I.: "Tipología legal de la firma electrónica en la Unión Europea", *Revista de la Contratación Electrónica*, núm. 23, Enero, 2002
- ALAMILLO DOMINGO, I.; URIOS APARASI, X: "Comentario crítico de la Ley 59/2003", *Revista de la Contratación Electrónica*, febrero, 2004, núm.46.
- ALBA, M.: "Necesidad para el comercio internacional de una regulación armonizada sobre documentos electrónicos negociables", CNUDMI, 28 de enero, 2011.
- ALLIANCE FOR GLOBAL BUSINESS: *A discussion paper on trade-related aspects of electronic commerce in response to the WTO´s e-commerce work programme*, abril, 1999.
- ÁLVAREZ CIENFUEGOS SUAREZ, M. Jª: *La firma electrónica y el comercio electrónico en España. Comentarios a la legislación vigente*, Madrid, 2000. Pág. 79.
- ÁLVAREZ GONZÁLEZ, S.: "Jurisprudencia española y comunitaria de derecho internacional privado", *Revista de Derecho Internacional Española*, 2005, vol. LVII, 2.
- ÁLVAREZ RODRÍGUEZ, M.: "El DNIe español como puerta de entrada a servicios de Administración electrónica en Europa: Proyecto STORK", *Recurso en línea*.

- APEC: *2001 Leaders' Declaration: Shanghai Declaration - Meeting New Challenges in the New Century (Action Agenda for the New Economy). Appendix 2 - e-APEC Strategy*, Shanghai, China, 21 de octubre 2001.
- APEC: *APEC Economic Leaders' Declaration: Delivering to the Community. Annex 1 - Action Agenda for New Economy*, Brunei, 16 de noviembre 2000.
- APEC: *Assessment Report on Paperless Trading of APEC Economies*, Pekín, 2005.
- APEC: *TEL 1/2007: Information Security certification Assessement Guide*, mayo de 2007, núm. 207-TC- 01.2.
- ARIAS POU, Mª: *Manual práctico de comercio electrónico*, Madrid, 2006.
- ARMENTA DEU, T.: *Lecciones de Derecho Procesal Civil*, Madrid, 2010.
- ASEAN: *Memorandum of Understanding between the Governments of the Member Countries of the Association of Southeast AsiaNations and the Government of Australia on the ASEAN-Australia Economic Cooperation Programme (AAECP)*, Bangkok, Thailand, 27 July 1999.
- BALBONI, P.: "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information & Communications Technology Law*, núm.3, vol. 4, 2004.
- BEAUMONT, P.; YÜRSEL, B.: "La reforma del Reglamento de Bruselas I sobre acuerdos de sumisión y la preparación para la ratificación por la UE del Convenio de la Haya sobre acuerdos de elección de foro", en *Anuario español de derecho internacional privado*, tomo IX, 2009.
- BERCOVITZ RODRIGUEZZ CANO, R.: *Comentarios al Código civil*, Valencia, 2013.
- BIEREKOVEN, C; BAZIN, P; y KOZLOWSKI, T.: "Electronic Signature in Germany, French and Polish Law Perspective", Digital evidence and electronic signature law review**,** octubre, 2004, núm. 1.

- BLANCHETTE, J.L.: "Defining Electronic Authenticity: An Interdisciplinary Journey", *Conferencia internacional sobre sistemas y redes fiables,* Florencia, 28 de junio-1 de julio, 2004.
- BLOCHER, W.: "Zur Haftung des Zertifizierungsdiensteanbieters nach S 11 Signaturgesetz 2001", *Blocher: Zur Haftung des Zertifizierungsdiensteanbieters,* 2007.
- BLYTHE, S.E.: "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce", *Chicago-Kent Journal of Intellectual Property*, vol. 7, núm.1, 2000.
- BONET NAVARRO, J.: *La prueba en el proceso civil: cuestiones fundamentales,* Madrid, 2009.
- BORGOÑO TORREALBA, J.L.: "Arbitraje Comercial Internacional online", *Anuario Español de Derecho Internacional (AEID),* núm. 23, 2007.
- BORRÁS, A...: "La aplicación del Reglamento Bruselas I a domiciliados en terceros estados: los trabajos del grupo europeo de derecho internacional privado", en *Anuario español de derecho internacional privado,* Tomo X, 2010.
- BORRELL, J.: *Derecho notarial*, Valencia, 2011.
- BRAZEL, L: *Electronic Signatures, Law and Regulation,* Oxford, 2004.
- BUCHMAM, J: "Post-quantum signatures", *Invited talk Darmstadt University of Technology. Germany,* 30 de septiembre de 2004.
- BUCKLEY, J. S.; TANK, M., BUCKLEY KOLAR LLP: *Electronic Signatures and Records Under ESIGN, UETA and SPeRS,* 2007.
- CALVO CARAVACA, A. L. Y AREAL LUDEÑA, S.: *Comentarios actuales al derecho mercantil internacional,* Madrid, 2005.
- CALVO CARAVACA, A. L. y CARRASCOSA GONZÁLEZ, J.: *Derecho Internacional Privado,* Granada, 2012.
- CALVO CARAVACA, A. L. y J. CARRASCOSA GONZALEZ, J.: *Conflictos de Leyes y conflictos de jurisdicciones en internet*, Madrid, 2001.

- CARAYANNIS, E. G.; TUNER, E.: "Innovation diffusion and technology acceptance: The case of PKI technology", *Review ScienceDirect: Technovation*, marzo, 2002.
- CAROLINA, R; LYFORD, J; LYONS, T.*:* "THE Intersection of Public Key Infrastructures and the Law", *Information Security Technical Report*, 2000, vol. 5, nº 4.
- CARTA DE LOS DERECHOS FUNDAMENTALES RECONOCE UNA SERIE DE DERECHOS PERSONALES, CIVILES, POLÍTICOS, ECONÓMICOS Y SOCIALES DE LOS CIUDADANOS Y RESIDENTES DE LA UE, CONSAGRÁNDOLOS EN LA LEGISLACIÓN COMUNITARIA.
- CENTRO LATINOAMERICANO DE ADMINISTRACIÓN Y DESARROLLO (CLAD): "Marco para la identificación electrónica social iberoamericana", *Aprobado por la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado*, Asunción, 30 junio – 1 julio, 2011.
- CHISSICK, C.: *Electronic commerce: law and practice*, Londres, 2002.
- CLIFFFORD NEUMAN, B.; TS´O, T.: "Kerberos: An Authentication Service for Computer Networks", *IEEE Communications Magazine*, septiembre, 1994, vol.32, núm.9.
- CNUDMI /UNCITRAL: *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, 1999.
- CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMCE* (2001), Nueva York, 2001.
- CNUDMI/UNCITRAL: *A/CN. 9/ 483 - Informe del grupo de trabajo sobre comercio electrónico acerca de la labor de su 37º período de sesiones*, Viena, 6 de octubre de 2000.
- CNUDMI/UNCITRAL: *A/CN.9/484 - Informe del Grupo de Trabajo sobre Comercio Electrónico acerca de 38º período de sesiones*, Nueva York, 12 a 23 de marzo de 2001.

- CNUDMI/UNCITRAL: *A/CN.9/681/Add.1 - Posible labor futura en materia de comercio electrónico: propuesta de los Estados Unidos de América sobre los documentos electrónicos transferibles*, Viena, 29 de junio a 17 de julio de 2009.
- CNUDMI/UNCITRAL: *A/CN.9/681/Add.2 - Posible labor futura en materia de comercio electrónico: propuesta de los Estados Unidos de América sobre la solución de controversias por vía informática*, Viena, 29 de junio a 17 de julio de 2009.
- CNUDMI/UNCITRAL: *A/CN.9/682 - Propuesta de la Delegación Española para los trabajos futuros del Grupo de Trabajo IV de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*, Viena, 29 de junio a 17 de julio de 2009.
- CNUDMI/UNCITRAL: *A/CN.9/737 - Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 45º período de sesiones*, Nueva York, 18 de junio a 6 de julio de 2012.
- CNUDMI/UNCITRAL: A/CN.9/WG.III/WP.127 - Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico, Grupo de Trabajo III (Solución de Controversias en Línea), 29° período de sesiones, Nueva York, 24 a 28 de marzo de 2014.
- CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.113 - Aspectos jurídicos del comercio electrónico: Cláusulas contractuales 2004 de la CCI para el comercio electrónico (ICC eTerms 2004). Guía de la CCI para la contratación electrónica*, Viena, 11 a 22 de octubre de 2004.
- CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.119 - Cuestiones jurídicas relativas al empleo de documentos electrónicos transferibles: propuesta de los Gobiernos de Colombia, España y los Estados Unidos*, Viena, 29 de octubre a 2 de noviembre de 2012.
- CNUDMI/UNCITRAL: A/CN.9/WG.IV/WP.120 - *Panorama general de la gestión de la identidad digital. Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Viena, 29 de octubre a 2 de noviembre de 2012.
- CNUDMI/UNCITRAL: *Anuario volumen XXXVI: 2005*, Nueva York, 2010.

- CNUDMI/UNCITRAL: *Anuario: volumen XXIX: 1998,* Nueva York, 2001.
- CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica,* Viena, 2009.
- CNUDMI/UNCITRAL: *Guía jurídica para la incorporación al derecho interno de la LMFE*, Nueva York, 2002.
- CNUDMI/UNCITRAL: *Jurisprudencia relativa a los textos de la CNUDMI (CLOUT).*
- CNUDMI/UNCITRAL: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007.
- CNUDMI UNCITRAL: *A/CN.9/WG.IV/WP.129 - Programa provisional anotado,* Viena, 10 a 14 de noviembre de 2014.
- CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.130 - Proyecto de disposiciones sobre los documentos electrónicos transferibles*, Viena, 10 a 14 de noviembre de 2014.
- CNUDMI/UNCITRAL: *A/CN.9/WG.IV/WP.130/Add.1 - Proyecto de disposiciones sobre los documentos electrónicos Transferibles*, Viena, 10 a 14 de noviembre de 2014.
- COCHA CANTÍ, H (Dirs.); LÓPEZ AYLLÓN, S.; TACHER EPELSTEIN, L. (Coords.): *Transparentar al Estado: la experiencia mexicana de acceso a la información,* México DF, 2005.
- COMISIÓN EUROPEA: *Libro blanco del comercio (COM(1999) 6 final)*, Bruselas, 27 de enero de 1999.
- COMISIÓN EUROPEA: *Comunicación de la Comisión de 18 de abril de 1997: Una iniciativa europea en el sector del comercio electrónico (COM (97)157 final– no publicada en el Diario Oficial)*, Bruselas, 16 de abril de 1997.
- COMISIÓN EUROPEA – MERCOSUR. Documento estratégico regional 2007 – 2013. (2/8/2007 – E/2007/1640).

- COMISIÓN EUROPEA: *Agenda Digital: la Comisión esboza un plan de acción para potenciar la prosperidad y el bienestar europeos (MEMO/10/200)*, Bruselas, 19 de mayo de 2010.
- COMISIÓN EUROPEA: *Agenda Digital: nuevo Reglamento para hacer posible la firma electrónica transfronteriza y sacar más ventaja de la identificación electrónica en el mercado único digital*, Comunicado de prensa, Bruselas, 4 de junio de 2012.
- COMISIÓN EUROPEA: *Comunicación de la Comisión a tenor del apartado 3 del artículo 19 del Reglamento nº 17 del Consejo relativa al asunto COMP/27.462 – Identrus (2000/C 231/03)*, DOUE, núm.3, 11 de agosto 2000.
- COMISIÓN EUROPEA: *Comunicación relativa a la mejora del acceso de los consumidores a mecanismos alternativos de solución de litigios (COM/2001/0161 final)*, Bruselas, 4 de abril de 2001.
- COMISIÓN EUROPEA: Decisión de la Comisión de 31 de Julio de 2001 relativa a un procedimiento con arreglo al Artículo del Tratado 81 del Tratado CE y el Artículo 53 del Acuerdo EEE. (Asunto COMP/37.462 – Identrus).
- COMISIÓN EUROPEA: *Dictamen de la comision con arreglo a la letra c) del apartado 2 del artículo 251 del Tratado CE, sobre las enmiendas del Parlamento Europeo a la posición común del Consejo sobre la Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO por la que se establece un marco comunitario para la firma electrónica POR EL QUE SE MODIFICA LA PROPUESTA DE LA COMISION con arreglo al apartado 2 del artículo 250 del Tratado CE (COM (1999) 626 final 1998/0191 - COD)*, Bruselas, 26 de noviembre de 1999.
- COMISIÓN EUROPEA: *Doce líneas de actuación para el mercado único de 2012: juntos para un nuevo crecimiento (IP/11/469)*, Bruselas, 13 de abril de 2011.
- COMISIÓN EUROPEA: *Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y de servicios de confianza para las transacciones electrónicas en el mercado interior*, Bruselas, 4 de junio de 2012, COM (2012) 238 final.

- COMISIÓN EUROPEA: *Informe sobre la aplicación de la Directiva 1999/93/CE*, Bruselas, 2008.
- COMISIÓN EUROPEA: *Una Agenda Digital para Europa: iniciativas clave (IP/10/581)*, Bruselas, 19 de mayo 2010; COMISIÓN EUROPEA: *Una Agenda Digital para Europa: ¿en qué me beneficia? (MEMO/10/199*), Bruselas, 19 de mayo de 2010.
- COMISIÓN EURPEA: *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al COMITÉ Económico y Social Europeo y al Comité de las Regiones (COM (2008) 798 final): sobre el Plan de acción de sobre firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único,* Bruselas, 28 de Noviembre de 2008.
- COMISIÓN EURPEA: *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al COMITÉ Económico y Social Europeo y al Comité de las Regiones (COM (2008) 798 final): sobre el Plan de acción de sobre firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único,* Bruselas, 28 de Noviembre de 2008.
- CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Conclusiones y Recomendaciones adoptadas por la Comisión Especial sobre el Funcionamiento práctico de los Convenios sobre Apostilla, la Obtención de Pruebas y la Notificación,* octubre/noviembre de 2003.
- CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Geneva round table on Electronic Commerce and Private International Law,* Comunicado de prensa, septiembre de 1999.
- CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO: *Reseña sobre el Convenio de la Haya sobre Acuerdos de Elección de Foro*, La Haya, 2009.
- CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO; CÁMARA INTERNACIONAL DE COMERCIO; MINISTERIO HOLANDÉS DE ASUNTOS ECONÓMICO INTERNATIONAL: *Conference on the Legal Aspects of an E-Commerce Transaction*, 26 y 27 octubre de 2004.

- CONFERENCIA IBEROAMERICANA DE MINISTROS/-AS DE ADMINISTRACIONES PÚBLICAS Y REFORMAS DEL ESTADOS: *Marco para la identificación electrónica social iberoamericana*, Asunción, Paraguay, 2011.
- CONSEJO DE ESTADO: *Doctrina legal,* Boletín Oficial del Estado, Madrid, 2006.
- CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA): *Principios y Recomendaciones preliminares sobre la protección de datos (la protección de datos personales)*, Washington, 2011.
- CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA): Ley Modelo Interamericana sobre acceso a la información pública, l8 de junio de 2010.
- COTINO HUESO, L.: *Consumidores y usuarios ante las nuevas tecnologías,* Valencia, 2008
- COUTO CALVIÑO, R.: "Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación", *Revista electrónica de la Contratación*, núm. 83, Junio, 2007.
- COUTO CALVIÑO, R.: *Servicios de certificación de firma electrónica y libre competencia*, Granada, 2008.
- CRUZ RIVERO, D. "Contratación electrónica con consumidores", *Revista de la contratación electrónica*, Nº 109, 2009.
- CRUZ RIVERO, D.: "Análisis del concepto de firma electrónica como equivalente de la firma manuscrita", Revista de la Contratación Electrónica, núm. 60, mayo, 2005.
- CRUZ RIVERO, D.: "Firma electrónica y documento electrónico en la nueva regulación alemana: su adaptación a la normativa comunitaria", *Revista de la Contratación Electrónica,* marzo, 2002.
- CRUZ RIVERO, D.: *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de Diciembre, de firma electrónica*, Madrid, 2006.

- CRUZ RIVERO: "El DNI electrónico y el mercado de entidades de certificación", *Revista Electrónica de la Contratación*, 2006.
- CRUZ RIVRO, D.: *Eficacia formal y probatoria de la firma electrónica*, Madrid, 2006.
- CURRY, S.: *"*Washington's electronic signature Act: an anachronism in the new millennium", *Washington Law Review*, junio, 2013, vol. 88, núm. 2.
- CUTHBERTSON, A., "Estonia First Country to Offer E-Residency Digital", *International Business Times*.
- DAVARA RODRÍGUEZ, M. A.: *La protección de datos en Europa*, Madrid, 1998.
- DAVIES, M.: "Time to Change the Federal Forum Non Conveniens Analysis", *LexisNexis Review,* 2002, núm.309.
- DAVINSON, A.: *The law of electronic commerce*, Cambridge, 2009.
- DE MIGUEL ASENSIO, P. A.: *Derecho Privado de Internet*, Madrid, 2002.
- DE MIGUEL ASENSIO, P. A.: *Derecho privado de Internet*, Madrid, 2011.
- DE MIGUEL ASENSIO, P.A.: "Regulación de la firma electrónica: balance y perspectiva", *Direito da Sociedade da Informaçao*, Coímbra, 2004.
- DEPARTMENT OF COMMERCE; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (USA): Report *to Congress: Electronic Signature in Global National Act. Section 105 (a)*, junio de 2001.
- DEPARTMENT OF TRADE AND INDUSTRY: *Achieving best practice in your business: Information Security: Guide to the Electronic Communications Act 2000*, Londres, 2004.
- DIAGO DIAGO, Mª.P.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario LA LEY*, núm. 8432, 2014.
- DÍAZ MORENO, A.: "Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica", *Revista de la Contratación Electrónica*, núm. 2, Febrero, 2000.

- DÍEZ PICAZO, L.; GULLÓN, A.: *Sistema de Derecho Civil (Volumen I)*, Madrid, 2001.
- DORAL, A.: *Seguridad en internet y medios de pago*, Madrid, 2002.
- ELECTRONIC COMMERCE EXPERT GROUP TO THE ATTORNEY GENERAL: *Electronic Commerce: Building the Legal Framework*, 31 de marzo de 1998.
- ELECTRONIC PRIVACY INFORMATION CENTER: *Real ID implementation review: few benefits, staggering costs. Analysis of the department of homeland security's national id program electronic privacy information center*, mayo, 2008.
- ELECTRONIC TRANSACTIONS ACT 2010 (ACT 16 OF 2010): *Appointment of Controller.*
- ERDOZÁIN LÓPEZ, J. C.: "Firma electrónica, aspectos procesales, valor probatorio modelos de responsabilidad de los prestadores de servicios de certificación", Revista Aranzadi Civil, abril, 2003.
- ESLER, B. W.: Lorraine v Markel: unnecessarily raising the standard for admissibility of electronic evidence", *Digital evidence and electronic signature law review,* octubre, 2007, núm. 4.
- ESTRELLA-FARIA, J.A.: "Legal Aspects of Electronic Commerce in International Trade (Part II) – Electronic Authentication ans Signature Methods: Legal Issues and Public Policy", *CNUDMI: Recursos en línea y transmisiones Web.*
- ETCHEVERRY R.A. Y ILLESCAS ORTIZ, R.: *Comercio electrónico: estructura operativa y jurídica,* Buenos Aires, 2010.
- ETEL RAPALLINI, L.: "La empresa y el arbitraje "on line" en el comercio internacional", *Derecho Internacional,* ANALES Nº 42 - Facultad de Cs. Jurídicas y Sociales. U.n.l.p. 2012.
- FABIO PIACENZA, D.: "Habeas Data derecho a la información", *AR. Revista de Derecho Informático,* núm.34, 2010.

- FAJARDO LÓPEZ, L.: *Firma electrónica en el Derecho Privado,* Madrid, 2005.
- FEDELSTEIN DE CARDENAS, S. L.; SCOTI, L. B.: *Contratación electrónica internacional: una mirada desde el derecho internacional privado,* Buenos Aires, 2008.
- FEDERAL TRADE COMMISSION AND DEPARTMENT Of COMMERCE*: Electronic Signature in Global and National Commerce Act. The Consumer Consent Provision in Section 101 (c) (1) (c) (ii).* junio de 2001.
- FELDESTEIN DE CARDENAS, S. L.: "El Derecho Internacional Privado y los procesos de integración regional", *Revista Forense del temas de Derecho Privado, Buenos Aires,* 2000.
- FELDESTEIN DE CARDENAS, S. L.; COODS. ANDREA MEDINA, F.; SOFIA RODRIGUEZ, M.; Y, BEATRIZ SCOTTI, L.: *Contratación electrónica internacional: una mirada desde el Derecho Internacional Privado,* Buenos Aires, 2008.
- FEN LIM, Y.: "Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability", *Singapore Journal of International & Comparative Law*, núm. 7, 2007.
- FERNÁNDEZ – ARROYO, D.P. Y MORENO RODRÍGUEZ, J. A.: *Derecho internacional privado – Derecho de la libertad y el respeto mutuo. Ensayos a la memoria de Tatiana B. de Maekelt*, CEDEP/ASADIP, Asunción, 2010.
- FERNÁNDEZ-BALLESTEROS LÓPEZ, M. A.; RIFÁ SOLER, J. Mª. VALLS GOMBAU, J.: *Comentarios a la nueva Ley de enjuiciamiento civil: volumen II*, Barcelona, 2001.
- FORDER, J.: "The inadequate legislative response to e-signature", *ScienceDirect Review*, vol. 26, 2010.
- FOX, W. F.: "The international Chamber of Commerce´s GUIDEC principles: private sector rules for digital signatures", *The International Lawer,* Vol. 35 – 1, 2001.
- FRANCH QUIRALTE, E.: "La representación en los negocios jurídicos", *Registradores y Notarios*, 9 de abril de 2003.

- FROOMKIN, A. M.: "Creating a viral federal privacy standard", *Boston College Law Review*, 2006.
- GAMERO, E.: "Interoperability and eGovernment: A Legal Approach to the European Union and Spanish Models", *Social Science Computer Review*, 28 February 2011.
- GARCÍA DE ENTERRÍA: en *La encrucijada constitucional de la Unión Europea*, Madrid, 2002.
- GARCÍA MAS, F. J.: "La firma electrónica de las personas físicas: comentario al art. 7 de la Ley 59/2003, de 19 de diciembre, sobre firma electrónica", *Actualidad civil*, año 2005 – 2.
- GOMES DE ANDRADE, N. N.: "Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID", *ScienceDirect Review*, vol. 28, núm. 2, 2012.
- GOVERNMENT UNIT, DG INFORMATION SOCIETY AND MEDIA, EUROPEAN COMMISSION: *The Modinis IDM Study Team: Modinis Study on Identity Management in eGovernment:Common Terminological Framework for Interoperable Electronic Identity Management*, Version 2.01, 23 de noviembre de 2005.
- GREGORY, J.D.: "Must e-signature be reliable?" *Digital evidence and electronic signature law review*, octubre, 2013, núm. 10.
- GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET (IETF): *Internet Security Glossary, RFC 2828, IETF Network Working Group*, mayo de 2000.
- GRUPO DE TRABAJO DE TELECOMUNICACIONES E INFORMACIÓN: *Electronic Authentication: Issues Relating to Its Selection and Use*, diciembre, 2002.
- GUERRERO LEBRÓN, Mª J.: "El crédito documentario electrónico y su nueva regulación", *Revista de la Contratación Electrónica*, Núm. 34, 2002.
- HATFIELD, P.; CASAMENTO, G.: "The essential elements of an effective electronic signature process", *Digital evidence and electronic signature law review*, octubre, 2009, núm. 6.

- HEDLEY, S.: *The Law of Electronic Commerce and the Internet in the UK and Irland*, Londres, 2006.
- HILLEBRAND, G and SAUNDERS, M.: *E-Sing and UETA, what should states do now?* Consumers Union, 2006.
- HINDELANG, S.: "No remedy for dissapointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Informatica, Law and Technology*, nº 1, 2002.
- HOMELAND SECURITY: *REAL ID enforcement in brief*, 5 de febrero de 2014.
- HUERTAS VIESCA, M. I. y RODRÍGUEZ RUÍZ DE VILLA, D.: *Los prestadores de servicios de certificación en la contratación electrónica*, Madrid, 2001.
- IDA SINGAPORE: *Application form for accreditation / renewal of accreditation of certification authority.*
- IDA SINGAPORE; ATTORMEY GENERAL'S CHAMBERS: *Joint IDA-AGC review of electronic, transactions act proposed amendments 2009*, LRRD No.1/2009, 30 de junio de 2009.
- IDABC: *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*.
- ILLESCAS ORTIZ, R.: "La firma electrónica y el R.D. Ley 14/1999, de 17 de septiembre", *Derecho de los negocios*, núm. 109, octubre 1999.
- ILLESCAS ORTÍZ, R.: *Derecho de la Contratación Electrónica*, Madrid, 2009.
- ILLESCAS ORTÍZ, R.; RAMOS HERRANZ, I.: *Derecho del comercio electrónico*, Buenos Aires, 2010
- ILLESCAS, R; CREMADES, J.; FERNÁNDEZ-ORDÓÑEZ, M. A: *Régimen jurídico de internet* Madrid, 2002.
- INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: *IEEE Standard Computer Dictionary A Compilation of IEEE Standard Computer Glossaries. Standards coordinatingcodttee of the EEE computer Society*, Nueva York, 1990.

- INTVEN, H.; PFOHL, R.; SLUSARCHUK, C.: "Legal and regulatory aspects of e-commerce and the internet", *The World Bank Legal Review. Law and Justice for Development*, núm.1, 2003.
- IPR HELPDESK: *"Estudio sobre firma electrónica"*, Proyecto financiado por la Comisión Europea. Dirección General de Empresas e Industria en el sexto programa Marca sobre IDT de la Unión Europea.
- JOS DUMORTIER, J.; VANEZANDE, N.: "Trust in the proposed EU regulation on trust services?" *Computer Law & Security Review*, Vol. 28, núm. 5, octubre, 2012.
- KAH LENG, T.: "Have you signed your electronic contract?" *Computer Law and Security Review*, febrero, 2011, vol. 27, nº 1.
- KIEFER, B. K.: "ABA draft PKI assessment guidelines: building consensus on PKI assessment: release of the ABA draft PKI assessment guidelines for public comment", *Computer Law&Security Review*, Vol. 17, Num. 6, 2003.
- KIMMEL, F. P.: "Beweiskraft der elektronischen signatur im zivilprozess in deutschland und österreich", *Abschlussarbeit im rahmen des ergänzungsstudiengangs rechtsinformatik an der Universität Hannover*, 11 de Julio de 2003.
- KISSWAN, N. M.; AL-BAKR, A.: "Regulating the use of electronic signatures given the changing face of contracts", *MqJBL*, vol.7, 2007.
- KNAUS, J.P.; FOLEY, T. E.: "Electronic Records & Signatures: The federal E-Sign Act and Michigan UETA place them on legal par with their paper and ink counterparts", *Michigan Bar Journal*, Julio, 2001.
- KOMMERSKOLLEGIUM/SWEDISH NATIONAL BOARD OF TRADE: "E-invoicing in cross-border trade", *UNCITRAL Colloquium on Electronic Commerce*, 14-16 de febrero de 2011, Neva York, pág. 7.
- KRAWCZYK, P.: "When the EU qualified electronic signature becomes an information services preventer", *Digital evidence and electronic signature law review*, octubre, 2010, núm. 7..
- KUNER, C; BARCELO, R; BARKER, S.; GREENWALD, E.: *An Analysis of International Electronic and Digital Signature Implementation Initiatives: A*

Study Prepared for the Internet Law & Policy Forum (ILPF), A Study Prepared for the Internet Law & Policy Forum (ILPF), septiembre, 2000.

- KUTYŁOWSK, M.; BŁASKIEWICZ, P.; KRZYWIECK, L.; KUBIAK, P.; PALUSZYNSKI, W.; TABOR, M.: "Technical and Legal Meaning of "Sole Control" – Towards Verifiability in Signing Systems", *Wrocław University of Technology, Trusted Information Consulting, Warsaw,* 2011.
- LAFUENTE SUÁREZ, M: "Análisis de la Ley 59/2003, de firma electrónica, tras dos años de vigencia: problemas no resueltos en torno a los certificados de firma electrónica", *Revista Aranzadi de Derecho de las Nuevas Tecnologías,* 2006 - 2, núm. 11.
- LARRAZABAL BASAÑEZ, S.: "La protección de los consumidores en la carta, de los Derechos Fundamentales de la Unión Europea", *Jado boletín de la Academia Vasca de Derecho,* 2011, núm.22.
- LEVIN, R.: RESNITZKY, U.: "El libro blanco de la Firma Digital: la mejor aproximación a la firma digital basada en PKI", *Arx: Algorithic Research,* enero, 2005.
- LISI, A.: *I Contrati di Internet: Sottoscrizione del consumatore, privacy e mezzi di pagamento,* Milán, 2006.
- LODDER, A.R.; KASPERSEN, H. W. K.: *eDirective: Guides to European Union Law on eCommerce,* La Hague, 2002.
- LOPEZ GALIANO PERONA, J.: "Firma electrónica de la persona jurídica: una alteración del sistema clásico de representación", ,*Boletín del Ministerio de Justicia,* año LIX, 15 de octubre de 2005, boletín núm. 1999, págs.3887 – 3905.
- LÓPEZ JIMENEZ, D.: "Iniciativas empresariales de regulación del comercio electrónico: el supuesto de la península Ibérica", *Revista Electrónica de la Contratación,* núm. 114, 2011.
- LÓPEZ, A.; MONTES, V.L.: *Derecho Civil. Parte general,* Valencia, 1998.
- LOW, R.; CHRISTENSEN, S.: "Electronic signatures and PKI frameworks in Australia", *Digital Evidence and Electronic Signature Law Review,* núm.1, octubre, 2004.

- LUDDY, B.: "Session IV: The International Single Window: A Legal Framework View of the Path to Paperless Global Trade Development", *UNCITRAL Colloquium on Electronic Commerce*, 14 - 16 de febrero, 2011, Nueva York.
- LYNCH, H. M.: "El documento y la firma digital en el Derecho Argentino", *Revista Anales de Legislación Argentina*, Boletín Informativo, 2001.
- M'CHIRGUI, Z.: "Smart card industry: a technological system", *Technovation Review*, núm.25, 2005.
- MADRID PARRA, A.: *"*Aspectos jurídicos de la identificación en el comercio electrónico", en *Derecho del Comercio Electrónico,* Valencia, 2001
- MADRID PARRA, A.: "Contratación electrónica y protección de datos personales", *Revista de la Contratación Electrónica*, 2008, núm. 94.
- MADRID PARRA, A.: "Contratos electrónicos y contratos informáticos", Revista de la Contratación Electrónica, núm.111, enero, 2011.
- MADRID PARRA, A.: "Electronificación del arbitraje", *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Riedpa)*, núm. 2, 2011.
- MADRID PARRA, A.: "La identificación electrónica", *Revista de la Contratación Electrónica*, Abril, núm. 15, 2001.
- MADRID PARRA, A.: "Ley modelo de la CNUDMI/UNCITRAL para las firmas electrónicas", *Revista Aranzadi de Derecho Patrimonial,* núm. 11, 2003.
- MADRID PARRA, A.: "Regulación internacional del comercio electrónico: examen comparado de las leyes modelo de UNCITRAL", *Revista Aranzadi de Derecho de las Nuevas Tecnologías*, núm. 2, 2003.
- MADRID PARRA, A.: "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil***,** núm.34, 2001.
- MADRID PARRA, A.: Firmas digitales y entidades de certificación, a examen en la CNUDMI/UNCITRAL, *Revista de Actualidad Informática Aranzadi*., julio de 1997.

- MADRID PARRA, A.: Lento caminar hacia una posible convención sobre contratación electrónica", *Revista de la Contratación Electrónica*, núm. 49, 2004.
- MADRID PARRA, A.: "Directiva 2013/11 (ADR) y Reglamento 524/2013 (ODR): Una apuesta europea por la solución alternativa de litigios y en pro del comercio electrónico transfronterizo", *Spain Arbitration Review. Revista del Club Español del Arbitraje*, nº. 18, 2013.
- MÁRQUEZ LOBILLO, P.: "Prestación de servicios de certificación en la LFE", *Revista de la Contratación Electrónica*, núm. 47, Marzo, 2004.
- MARTÍNEZ NADAL, A.: "Comentarios sobre la regulación de la firma electrónica", *Partida doble*, núm. 106, 1999.
- MARTÍNEZ NADAL, A.: *Comercio electrónico, firma electrónica y autoridades de certificación*, Madrid, 2000.
- MARTINEZ NADAL, A.: *Cometarios a la ley 59/2003 de Firma Electrónica*, Madrid, 2009.
- MARTÍNEZ NADAL, A.; FERRER, J.L.: "El problema temporal del sistema de certificados en el comercio electrónico", *Revista de la Contratación Electrónica*, enero 2001, núm. 1.
- MARTÍNEZ USERO, M. A.; LARA NAVARRA, P.: *La interoperabilidad de la información, Barcelona*, 2007.
- MARTORELL ZULUETA, P. (Coord.): *Código civil: jurisprudencia sistematizada*, Valencia, 2011.
- MASON, S.: "Electronic Signatures - Evidence: the evidential issues relating to electronic signatures", *Computer Law & Security Review,* mayo, 2002, vol. 18, núm. 3.
- MASON, S.: "Validating identity for the electronic environment", *Computer Law & Security Review,* mayo, 2004, vol.20, núm. 3, vol. 3.
- MASON, S.: *Electronic signature in Law,* Cambridge, 2012.
- MATA Y MARTÍN, R. M. (Dir.) JAVATO MARTÍN, A. Mª (Coord.): *Los medios electrónicos de pago: problemas jurídicos*, Madrid, 2007.

- MATTA, L. F.: "Contestación al discurso de instalación de la Profesora Olga Soler Bonnin", artículo correspondiente a *Real Academia de Jurisprudencia y Legislación*, Puerto Rico, 2013.
- MAZO PORTERA, A. Y RAMOS SUAREZ, F. Mª (Dir.): *La protección de datos en la gestión de empresas,* Navarra, 2004.
- MCKENNA, P.: "The probative value of digital certificates: Information Assurance is critical to e-Identity Assurance", *Digital evidence and electronic signature law review*, octubre, 2004.
- MEDINA ALCOZ, Mª: *La culpa de la víctima en la producción del daño*, Madrid, 2003.
- MINYIAN WANG: "Do the regulations on electronic signature facilitate international electronic commerce? A critical review", *Science Direct Review*, enero, 2007.
- MLA BUSINESS/TECHNOLOGY EDITORS: *Identrus, LLC to Acquire Digital Signature Trust; Merger Aligns U.S. Financial Services Community and TrustID with the Identrus Global Standard for Identity Authentication*, 2002.
- MONCAYO, VINUESSA, GUTIERREZ POSSE: *Derecho Internacional Público*, Buenos Aires, 1990
- MUN-CHO KIM:" Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea" *International Sociology*, junio, 2004.
- MURAKAMI, T.; TAKAHASHI , K.: "A measure of information gained through biometric systems", *Image and Vision Computing*, 26 de diciembre 2013.
- NÖDLER, J. N.: "Legal Framework of Electronic Signatures in the European Union and Germany", *Seminar in Network Security Institute of Computer Science Georg-August-Universität Göttingen*, 20 de febrero, 2006.
- NORTON, W. K.: "Enforcing 'simple' electronic signatures in an international context", *Digital evidence and electronic signature law review*, octubre, 2012, núm. 9.

- NOTICIA SCIENCE DIRECT: "German ID card to promote e-commerce", *Card Technology Today*, julio – agosto, 2008, vol.20, núm.7.
- OCDE: "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, 2011 núm.196.
- OCDE: *The use of authentification across Borders in ORCD Countries*, Paris, 2005.
- OLIVA BLÁZQUEZ, F.: "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19.
- OMB; DEPARTMENTS OF COMMERCE, JUSTICE, AND TREASURY: G*uidance on implementng the Electronic Signatures in Global and National Commerce Act (E-SIGN)*.
- ORDUÑA MORENO, F. (DIR.), CAMPUZANO LAGUILLO, A.B.; PLAZA PENADÉS, J. (COORDS.): *Contratación y comercio electrónico*, Valencia, 2003.
- ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL: *Información sobre el borrador preliminar del Competencia y Resoluciones Judiciales Extranjeras en Materia Civil y Comercial*, Ginebra, 28 de septiembre de 1999.
- ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO, GRUPO DE TRABAJO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LA VIDA PRIVADA: *The use of Authentification across Borders in OECD Countries*, París, 2005.
- ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN (ISO): *Glossary of IT Security Terminology, SC 27 Standing Document 6*, 31 de marzo de 2002.
- ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS: Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, París, 2004.

- ORTEGA DÍAZ, J.F.*: La firma electrónica y el contrato de certificación electrónico*, Madrid, 2008.
- ORTELLS RAMOS, M.: *Derecho Procesal Civil*, Navarra, 2013.
- PAREJO NAVAJAS, T.: *"*Análisis de las figuras esenciales del régimen jurídico de la firma electrónica: la Ley 59/2003, 19 de diciembre, de firma electrónica", *Revista Electrónica de la Contratación*, núm. 70, 2006.
- PEÑA, M.: "Proyecto MERCOSUR Digital. Apoyando a la sociedad de la información del MERCOSUR", *en II Encuentro Regional Latino Americano y del Caribe sobre Ventanillas Únicas de Comercio Exterior: avances y retos, Chile*, diciembre de 2010.
- PERALES VISCASILLAS, Mª P.: "Publicidad y Formación del contrato: Convención de UNCITRAL sobre la utilización de las comunicaciones electrónicas en los contratos internacionales, 2005", *Revista Electrónica de la Contratación*, núm. 72, junio 2006.
- PEREZ PEREIRA, Mª.: *Firmas Electrónicas: Contratos y Responsabilidad Civil*, Navarra, 2009.
- PONTEN, J.: "Session IV: Single Window Solutions - Best Practice and Challenges for the Future", *UNCITRAL Colloquium on Electronic Commerce,* , Nueva York, 14 - 16 de febrero, 2011.
- PRICE, G: "The benefits and drawbacks of using electronic identities", *Information Security Technical Report*, mayo, 2008, vol. 13, núm, 2.
- REAL ACADEMIA DE LA LENGUA ESPAÑOLA: *Diccionario de la lengua española*, Madrid, 2001.
- REINIGER, R. T.: "The proposed international e-identity assurance standard for electronic notarization", *Digital evidence and electronic signature law review*, octubre, 2008, núm. 5.
- RIBAS ALEJANDRO, J.: *Aspectos jurídicos del comercio electrónico en Internet,* Elcano, 2002.
- RICÓN CARDENAS, E.*: Manual de Comercio Electrónico y de Internet*, Bogotá, 2006.

- RIGAUX, F.: *Derecho Internacional Privado: Parte General*, Madrid, 1985.
- RODRÍGUEZ ADRADOS, A.: "La firma electrónica", *Revista jurídica del Notariado*, núm. 35, 2000.
- RODRÍGUEZ BENOT, A.; YBARRA BORES, A.: "La determinación del ordenamiento aplicable a los contratos internacionales en un mercado globalizado: la experiencia europea", Congreso Internacional de Derecho Mercantil, Instituto de Investigaciones Jurídicas de la UNAM, del 8 al 10 de marzo de 2006.
- RODRIGUEZ LÓPEZ, A.: "Aspectos normativos de la factura electrónica o e-factura en el ámbito europeo", *Revista de la Contratación Electrónica*, año, 2012, núm. 117.
- ROSARIO RODRÍGUEZ, M. F.: "La protección de datos personales entre particulares: esbozos de un esquema de regulación y protección en México", *Derecho comparado de la información*, 2012, Núm.20.
- ROSELLO, C.; FINOCCHIARO, G.; TOSI, E.: *Trattato di diritto privato: diretto da Mario Bessone. Volume XXXII, Commercio Elettronico*, Torino, 2007.
- ROSSELLÓ MORENO, R.: *Comercio electrónico y la protección de los consumidores*, Barcelona, 2001.
- RÖSSLER, T.: "Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government", *Computer Law & Security Review*, 2008, vol. 24, núm. 5.
- RUBIO VÁZQUEZ, R.; RODRIGUEZ SAU, C.; MUÑOZ MUÑOZ, R.: *La firma electrónica: Aspectos Legales y Técnicos*, Barcelona, 2004.
- SALLINGS, W.: *Fundamentos de Seguridad en Redes: Aplicaciones y Estándares*, Madrid, 2004, págs. 55 y ss.
- SALVATORI, M.: "El Convenio sobre Acuerdos de Elección del Foro y el Reglamento Bruselas I: autonomía de la voluntad y procedimientos paralelos", en *Anuario español de derecho internacional privado*, tomo X, 2010.
- SÁNCHEZ REÍLLO, R.: "La normalización en el campo de la Identificación Biométrica", *Dintel*, septiembre, 2012.

- SANDOVAL LÓPEZ, R.: "Análisis de la Ley Nº 19.799, de Firma Electrónica de la República de Chile", *Revista de la Contratación Electrónica,* núm. 32, noviembre, 2002.
- SCHAPPER, P. R.; RIVOLTA, M.; LEIPOLD, K.: "Authentication: International scope and non discrimination in government commerce vs. PKI", *Digital evidence and electronic signature law review,* núm 2, octubre, 2005.
- SCHAPPER, P.R.; RIVOLTA, M.; VEIGA, J.: "Risk and law in authentication", *Digital evidence and electronic signature law review,* octubre, 2006, núm. 6.
- SCHEERES, J.: "ID Cards Are de Rigueur Worldwide", *Wired News,* 25 de septiembre de 2001.
- SCHEERES, J.: "ID Cards Are de Rigueur Worldwide", *Wired News,* 25 de septiembre de 2001.
- SCHWARTZ, J.: *Archives - E-Signatures Become Valid For Business,* Noticia The New York Times, publicada, el 2 de octubre de 2000.
- SEALED, DLA PIPER AND ACROSS COMMUNICATIONS*: Study on the standardisation aspects of eSignature,* Bruselas, 2007.
- SECURITY COMMITTEE ELECTRONIC COMMERCE AND INFORMATION TECHNOLOGY DIVISION SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION: *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, agosto, 1996.
- SECURITY COMMITTEE ELECTRONIC COMMERCE AND INFORMATION TECHNOLOGY DIVISION SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION: *PKI Assessment Guidelines*, mayo, 2003.
- SENG, D.: "The Singapore Electronic Transactions Act and the Hong Kong Electronic Transactions Ordinance", *Digital Evidence and Electronic Signature Law Review,* núm. 5, octubre, 2008.
- SIMMONS & SIMMONS: *E-Commerce Law: doing business online*, Bembridge.

- SMEDINGHOFF, T. J.: "Solving the legal challenges of trustworthy on line identity", *Computer Law & Security Review*, octubre, 2012, vol. 28, núm.5.
- SMEDINGHOFF. T. J.: *American Bar Association Identity Management Legal Task Force Meeting*, 10 – 12 diciembre, 2012.
- SOBEL, R.: "The Degradation of Political Identity under a National Identification System", *Boston University Journal of Science & Technology Law*, 2001.
- SORGE, C.: "The legal classification of identity-based signatures", *Computer Law & Security*, abril 2014, vol. 30, núm. 2.
- SPYRELLI, C.: "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", *Journal of Information, Technology and Law*, vol. 2002, núm. 2, 2002.
- SRIVASTAVA, A.: "Electronic signatures and security issues: An empirical study", *Computer Law & Security Review*, septiembre, 2009, vol. 25, núm.5, págs. 432 – 446.
- STALLINGS, W.: *Fundamento de seguridad en Redes: Aplicaciones y Estándares*, Madrid, 2010.
- STEPHEN E.; BLYTHE: "China's new electronic signature law and certification authority regulations: a catalyst for dramatic future growth of e-commerce", Chicago-Kent Journal of Intellectual Property, 2007.
- SUK-LEE, K.: "Surveillant institutional eyes in South Korea: from discipline to a digital grid of control, the information society", *The Center for Interdisciplinary Research (ZiF*), 10- 11 febrero de 2006.
- TAUBER, A; KUSTOR, P KARNING, B: "Cross border certified electronic mailing: A European perspective" *Computer&Law Security Review*, Vol. 29, núm. 1, febrero, 2013.
- TELECOMICATIONS POLICY: *How advanced are Italian regions in terms of public e-services? The construction of a composite indicator to analyze patterns of innovation diffusion in the public sector*, 28 de febrero de 2014.

- TER HAH LENG: "E – Commerce: new law on e- commerce: Singapore", *Review Computer Law & Sevurity Report*, 1999, núm. 1, vol. 15.
- THE WHITE HOUSE (Office of the Press Secretary): *Joint Statement from Australia and the United States on electronic commerce*, 30 de noviembre 1998.
- TOBIAS, M; THOMAS, O.: "Risk, responsibility and compliance in circles of Trust", *Computer Law & Security Review*, 2007, vol. 23, núm. 3.
- TOMÉ MUGURUZA, B.: "El plan de acción info XXI: la sociedad de la información para todos", LA *Estrategia de impulso: economía industrial*, 2001, núm.338.
- UN DEPARTMENT OF PUBLIC INFORMATION: Press Release. China, Singapore, Sri Lanka sign un Convention on Use of Electronic Communications in International Contracts, Nueva York, 6 de Julio de 2006.
- UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005. (ECE/ TRADE/352, July 2005).
- UNCTAD: Conferencia de las Naciones Unidas sobre comercio y desarrollo: Directrices de las Naciones Unidas para la protección del consumidor (ampliadas en 1999), Nueva York y Ginebra, 2001.
- UPCROFT, A.: "E-Commerce: Global or Local? An Australian Case Study",*Journal of Law, Information and Science*, 1999, núm.113.
- VALPUESTA FERNÁNDEZ, Mª R: *Derecho Civil. Obligaciones y Contratos*, Valencia, 1998.
- VIRILI, C.; CANTONI, C.: "The Italian legislation on digital signatures and the role of Italian banks as Certificate Authorities: A strategic analysis", *Banking (including Insurance Stream):E-Commerce Services.*WALKER, E. F.: *Practical Guide to E-Sign and Uniform Electronic Transaction Act*, 2002.
- WANG, M.: "Translation and introduction to the Electronic Signature Law of China", *Digital evidence and Electronic Signature Law Review*, núm. 2, octubre 2005.

- WÉRY, É.: *Facturer électroniquement: droits européen, français et belge*, 2007,Bruselas.
- WESTIN, R.A.: *International taxation of Electronic commerce*, La Hague, 2000.
- ZAPATERO MIGUEL, P.: "Sistemas jurídicos especiales", *Revista Española de Derecho Internacional*, Vol. LVII – 2005.